2025/327

5.3.2025

REGLAMENTO (UE) 2025/327 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 11 de febrero de 2025

relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular sus artículos 16 y 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo ([1]),

Visto el dictamen del Comité de las Regiones ([2]),

De conformidad con el procedimiento legislativo ordinario ([3]),

Considerando lo siguiente:

(1) El objetivo del presente Reglamento es crear el Espacio Europeo de Datos de Salud (EEDS) con el fin de mejorar el acceso por parte de las personas físicas a sus datos de salud electrónicos personales y su control de dichos datos, en el contexto de la asistencia sanitaria, así como de alcanzar mejor otros fines para los que se necesite el uso de datos de salud electrónicos en el sector de la asistencia sanitaria y en el sector asistencial que beneficiarían a la sociedad, como, por ejemplo, la investigación, la innovación, la formulación de políticas, la preparación y respuesta ante las amenazas para la salud, incluidas la prevención y respuesta ante futuras pandemias, la seguridad de los pacientes, la medicina personalizada, las estadísticas oficiales o las actividades de regulación. Además, la finalidad del presente Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico y técnico uniforme, en particular en lo que respecta al desarrollo, la comercialización y el uso de los sistemas de historia clínica electrónica (en lo sucesivo, «sistemas HCE») de conformidad con los valores de la Unión. El EEDS va a ser una pieza clave para la creación de una Unión Europea de la Salud fuerte y resiliente.

(2) La pandemia de COVID-19 puso de relieve la necesidad de tener acceso en el momento oportuno a datos de salud electrónicos de calidad para la preparación y respuesta ante las amenazas para la salud, así como para la prevención, el diagnóstico y tratamiento y el uso secundario de dichos datos de salud electrónicos. Disponer de tal acceso en el momento oportuno podría contribuir potencialmente, mediante una vigilancia y un seguimiento eficientes de la salud pública, a una gestión más eficaz de futuras pandemias, a una reducción de los costes y una mejora de la respuesta a las amenazas para la salud y, en última instancia, podría ayudar a salvar más vidas. En 2020, la Comisión adaptó de manera urgente su Sistema de Gestión Clínica de Pacientes, establecido por la Decisión de Ejecución (UE) 2019/1269 de la Comisión ([4]), para permitir a los Estados miembros compartir datos de salud electrónicos de los pacientes de COVID-19 que se desplazaban entre los prestadores de asistencia sanitaria y los Estados miembros durante el período álgido de dicha pandemia. Sin embargo, esta adaptación fue solo una solución de emergencia, que mostró la necesidad de un enfoque estructural y coherente a nivel de los Estados miembros y a nivel de la Unión, tanto para mejorar la disponibilidad de datos de salud electrónicos para la asistencia sanitaria, así como para facilitar el acceso a los datos de salud electrónicos a fin de orientar respuestas políticas eficaces y contribuir a normas estrictas en materia de salud humana.

(3) La crisis de la COVID-19 consolidó firmemente el trabajo de la red de sanidad electrónica, una red voluntaria de las autoridades responsables en materia de salud digital, como el principal pilar para el desarrollo de aplicaciones de rastreo de contactos y de alerta a contactos para dispositivos móviles, así como de los aspectos técnicos de los

([1]) DO C 486 de 21.12.2022, p. 123.
([2]) DO C 157 de 3.5.2023, p. 64.
([3]) Posición del Parlamento Europeo de 24 de abril de 2024 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 21 de enero de 2025.
([4]) Decisión de Ejecución (UE) 2019/1269 de la Comisión, de 26 de julio de 2019, que modifica la Decisión de Ejecución 2014/287/UE, por la que se fijan los criterios para la creación y evaluación de las redes europeas de referencia y de sus miembros, y se facilita el intercambio de información y conocimientos en materia de creación y evaluación de tales redes (DO L 200 de 29.7.2019, p. 35).

certificados COVID digitales de la UE. También destacó la necesidad de compartir datos de salud electrónicos que sean fáciles de encontrar, accesibles, interoperables y reutilizables (en lo sucesivo, «principios FAIR»), y de garantizar que los datos de salud electrónicos sean tan abiertos como sea posible, respetando al mismo tiempo el principio de minimización de datos tal como dispone el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([5]). Deben garantizarse las sinergias entre el EEDS, la Nube Europea de la Ciencia Abierta y las infraestructuras europeas de investigación, y deben extraerse lecciones de las soluciones de intercambio de datos desarrolladas en el marco de la plataforma europea de datos sobre la COVID-19.

(4) Habida cuenta del carácter sensible de los datos de salud electrónicos personales, el presente Reglamento pretende proporcionar salvaguardias suficientes, tanto a escala nacional como de la Unión, para garantizar un nivel elevado de protección, seguridad, confidencialidad y uso ético de los datos. Esas salvaguardias son necesarias para fomentar la confianza en la gestión segura de los datos de salud electrónicos de las personas físicas para un uso primario o para un uso secundario tal como se definen en el presente Reglamento.

(5) Al tratamiento de los datos de salud electrónicos personales se le aplican las disposiciones del Reglamento (UE) 2016/679 y, en el caso de las instituciones, órganos y organismos de la Unión, las del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([6]). Las referencias a las disposiciones del Reglamento (UE) 2016/679 deben entenderse también como referencias a las disposiciones correspondientes del Reglamento (UE) 2018/1725 para las instituciones, órganos y organismos de la Unión, cuando proceda.

(6) Cada vez más personas que viven en la Unión cruzan las fronteras nacionales para trabajar, estudiar, visitar a familiares o por otros motivos. Para facilitar el intercambio transfronterizo de datos de salud, y en consonancia con la necesidad de facultar a los ciudadanos, estos deben poder acceder a sus datos de salud en un formato electrónico que pueda ser reconocido y aceptado en toda la Unión. Dichos datos de salud electrónicos personales podrían incluir datos personales relacionados con la salud física o mental de las personas físicas, también los relacionados con la prestación de servicios de asistencia sanitaria, y que revelen información sobre su estado de salud, datos personales sobre las características genéticas heredadas o adquiridas de las personas físicas, que proporcionen información única sobre la fisiología o la salud de dichas personas físicas y que se deriven, en particular, del análisis de una muestra biológica de la persona física en cuestión, así como datos sobre factores determinantes de la salud, como los conductuales, los medioambientales y las influencias físicas, la asistencia médica y los factores sociales o educacionales. Los datos de salud electrónicos también incluyen los datos que han sido inicialmente recogidos con fines de investigación, estadísticos, de evaluación de las amenazas para la salud, de formulación de políticas o de regulación y debe ser posible ponerlos a disposición de conformidad con lo establecido en el presente Reglamento. Los datos de salud electrónicos consisten en todas esas categorías de datos, independientemente de que los proporcionen los interesados u otras personas físicas o jurídicas, como los profesionales sanitarios, o se traten en relación con la salud o el bienestar de las personas físicas, y deben incluir también los datos inferidos o derivados, como los diagnósticos, las pruebas y los exámenes médicos, así como los datos observados y registrados de forma automatizada.

(7) En los sistemas sanitarios, los datos de salud electrónicos personales suelen recogerse en historias clínicas electrónicas, que habitualmente contienen el historial médico de las personas físicas, los diagnósticos y tratamientos, los medicamentos, las alergias, las vacunas, así como las imágenes radiológicas, los resultados de laboratorio y otros datos médicos, distribuidos entre diferentes agentes del sistema sanitario, como médicos de familia, hospitales, farmacias o servicios asistenciales. Para que las personas físicas o los profesionales sanitarios puedan acceder a los datos de salud electrónicos, compartirlos y modificarlos, algunos Estados miembros han adoptado las medidas jurídicas y técnicas necesarias y han creado infraestructuras centralizadas que conectan los sistemas HCE utilizados por los prestadores de asistencia sanitaria y las personas físicas. Además, algunos Estados miembros proporcionan su apoyo a la creación por parte de los prestadores de asistencia sanitaria públicos y privados de espacios de datos de salud electrónicos personales que permitan la interoperabilidad entre los distintos prestadores de asistencia sanitaria. Varios Estados miembros también apoyan o prestan servicios de acceso a datos de salud electrónicos para pacientes y profesionales sanitarios, por ejemplo, a través de portales de pacientes o profesionales sanitarios. Dichos Estados miembros también han tomado medidas para garantizar que los sistemas HCE o las aplicaciones de bienestar puedan transmitir datos de salud electrónicos al sistema central de HCE, por ejemplo, proporcionando un sistema de certificación. Sin embargo, no todos los Estados miembros han puesto en marcha tales sistemas, y aquellos Estados miembros que los han aplicado lo han hecho de manera fragmentada. Con el fin de facilitar la libre circulación de los

([5]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

([6]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

datos de salud electrónicos personales en toda la Unión y evitar consecuencias negativas para los pacientes cuando reciban asistencia sanitaria en un contexto transfronterizo, es necesaria una acción de la Unión para mejorar el acceso de las personas físicas a sus propios datos de salud electrónicos personales y para facultarlas para compartirlos. A este respecto, deben tomarse medidas apropiadas a escala nacional y de la Unión como medios para reducir la fragmentación, la heterogeneidad y la división, y para crear un sistema de fácil utilización e intuitivo en todos los Estados miembros. Toda transformación digital en el sector de la asistencia sanitaria debe aspirar a ser inclusiva y beneficiar también a las personas físicas con capacidad limitada para acceder a los servicios digitales y utilizarlos, incluidas las personas con discapacidad.

(8) El Reglamento (UE) 2016/679 establece disposiciones específicas relativas a los derechos de las personas físicas en relación con el tratamiento de sus datos personales. El EEDS se basa en dichos derechos y complementa algunos de ellos aplicados a los datos de salud electrónicos personales. Esos derechos se aplican independientemente del Estado miembro en el que se traten los datos de salud electrónicos personales, el tipo de prestador de asistencia sanitaria, las fuentes de esos datos o el Estado miembro de afiliación de la persona física. Los derechos y disposiciones relacionados con el uso primario de los datos de salud electrónicos personales con arreglo al presente Reglamento se refieren a todas las categorías de dichos datos, con independencia de cómo se hayan recogido o de quién los haya proporcionado, el fundamento jurídico del tratamiento en virtud del Reglamento (UE) 2016/679, o de la condición del responsable del tratamiento como organización pública o privada. Los derechos adicionales de acceso y la portabilidad de los datos de salud electrónicos personales que dispone el presente Reglamento deben entenderse sin perjuicio de los derechos de acceso y portabilidad establecidos en el Reglamento (UE) 2016/679. Las personas físicas siguen disfrutando de esos derechos en las condiciones establecidas en ese Reglamento.

(9) Si bien los derechos que confiere el Reglamento (UE) 2016/679 deben seguir aplicándose, el derecho de acceso a los datos por parte de las personas físicas, establecido en el Reglamento (UE) 2016/679, debe seguir complementándose en el sector de la asistencia sanitaria. En virtud de dicho Reglamento, los responsables del tratamiento no tienen que proporcionar el acceso inmediatamente. El derecho de acceso a los datos de salud sigue aplicándose habitualmente en muchos lugares mediante el suministro de los datos de salud solicitados en formato papel o como documentos escaneados, lo que lleva mucho tiempo para el responsable del tratamiento, como un hospital u otro prestador de asistencia sanitaria que proporciona acceso. Dicha situación retrasa que las personas físicas accedan a los datos de salud y puede tener un impacto negativo en ellas si necesitan acceder inmediatamente debido a circunstancias urgentes relacionadas con su estado de salud. Por ello es necesario ofrecer a las personas físicas una manera más eficiente de acceder a sus propios datos de salud electrónicos personales. Deben tener derecho a acceder de forma gratuita e inmediata, respetando al mismo tiempo la necesaria viabilidad tecnológica, a las categorías prioritarias específicas de datos de salud electrónicos personales, como la historia clínica resumida del paciente, a través de un servicio de acceso a los datos de salud electrónicos. Ese derecho debe aplicarse independientemente del Estado miembro en el que se traten los datos de salud electrónicos personales, el tipo de prestador de asistencia sanitaria, las fuentes de datos o el Estado miembro de afiliación de la persona física. El alcance de ese derecho complementario establecido en virtud del presente Reglamento y las condiciones para ejercerlo difieren en determinados aspectos del derecho de acceso a los datos personales en virtud del Reglamento (UE) 2016/679, el cual abarca todos los datos personales en poder de un responsable del tratamiento y se ejerce contra un responsable del tratamiento individual, que dispone de un plazo máximo de un mes para responder a una petición. El derecho de acceso a los datos de salud electrónicos personales en virtud del presente Reglamento debe limitarse a las categorías de datos que entren en su ámbito de aplicación, ejercerse a través de un servicio de acceso a los datos de salud electrónicos y traer consigo una respuesta inmediata. Los derechos en virtud del Reglamento (UE) 2016/679 deben seguir aplicándose, permitiendo a las personas físicas beneficiarse de los derechos en virtud de ambos marcos jurídicos, en particular, el derecho a obtener una copia en papel de los datos de salud electrónicos.

(10) Debe considerarse que el acceso inmediato de las personas físicas a determinadas categorías de sus datos de salud electrónicos personales puede ser perjudicial para la seguridad de esas personas físicas o poco ético. Por ejemplo, podría ser poco ético informar a un paciente a través de un canal electrónico sobre un diagnóstico de una enfermedad incurable que probablemente sea terminal, en lugar de proporcionar esa información en primer lugar en una consulta con el paciente. Por lo tanto, debe ser posible retrasar la prestación del acceso a los datos de salud electrónicos personales en tales situaciones durante un período de tiempo limitado, por ejemplo, hasta el momento en que el profesional sanitario pueda explicar al paciente la situación. Los Estados miembros deben poder establecer tales excepciones cuando constituyan una medida necesaria y proporcionada en una sociedad democrática, de conformidad con las limitaciones establecidas en el artículo 23 del Reglamento (UE) 2016/679.

(11) El presente Reglamento no afecta a las competencias de los Estados miembros relativas al registro inicial de datos de salud electrónicos personales, como condicionar el registro de datos genéticos al consentimiento de la persona física u otras garantías. Los Estados miembros pueden exigir que esos datos se proporcionen en formato electrónico antes de la aplicación del presente Reglamento. Ello no debe afectar a la obligación de poner a disposición en formato

electrónico los datos de salud electrónicos personales registrados tras la fecha de aplicación del presente Reglamento.

(12) Para completar la información que esté a su disposición, las personas físicas deben poder añadir datos de salud electrónicos a sus HCE o almacenar información adicional en su historia clínica personal independiente a la que pueden acceder los profesionales sanitarios. Sin embargo, la información introducida por personas físicas podría no ser tan fiable como los datos de salud electrónicos introducidos y verificados por los profesionales sanitarios y no tiene el mismo valor clínico o legal que la información proporcionada por profesionales sanitarios. Por ello, los datos añadidos por las personas físicas en sus HCE deben distinguirse claramente de los datos proporcionados por los profesionales sanitarios. Esa posibilidad de que las personas físicas añadan y complementen datos de salud electrónicos personales no debe darles derecho a cambiar los datos de salud electrónicos personales proporcionados por los profesionales sanitarios.

(13) Permitir a las personas físicas un acceso más fácil y rápido a sus datos de salud electrónicos personales les permitirá detectar posibles errores, como información incorrecta o historias clínicas asignadas incorrectamente a pacientes. En tales casos, las personas físicas deben poder solicitar en línea la rectificación de los datos de salud electrónicos personales incorrectos, de forma inmediata y gratuita, a través de un servicio de acceso a datos de salud electrónicos. Esas solicitudes de rectificación de datos deben ser tratadas por los responsables del tratamiento de conformidad con el Reglamento (UE) 2016/679, con la participación, si es necesario, de profesionales sanitarios con una especialización pertinente y que sean responsables de dispensar el tratamiento a la persona física.

(14) En virtud del Reglamento (UE) 2016/679, el derecho a la portabilidad de los datos se limita a los datos tratados sobre la base del consentimiento o contrato y proporcionados por el interesado a un responsable del tratamiento. Asimismo, en virtud de dicho Reglamento, las personas físicas tienen derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro solo cuando sea técnicamente posible. Sin embargo, el Reglamento (UE) 2016/679 no impone la obligación de hacer técnicamente viable esa transmisión directa. El derecho a la portabilidad de datos debe complementarse en el marco del presente Reglamento, facultando así a las personas físicas para proporcionar acceso al menos a las categorías prioritarias de sus datos de salud electrónicos personales a los profesionales sanitarios de su elección, a intercambiar tales datos de salud con esos profesionales sanitarios y a descargar tales datos de salud. Además, las personas físicas deben tener derecho a solicitar a un prestador de asistencia sanitaria que transmita una parte de sus datos de salud electrónicos a un destinatario claramente identificado en el sector de la seguridad social o de los servicios de reembolso. Esa transferencia debe ser de un solo sentido.

(15) El marco establecido por el presente Reglamento debe basarse en el derecho a la portabilidad de los datos establecido en el Reglamento (UE) 2016/679, garantizando que las personas físicas, como interesados, puedan transmitir sus datos de salud electrónicos personales, incluidos los datos inferidos, en el formato europeo de intercambio de historias clínicas electrónicas, con independencia de la base jurídica para el tratamiento de los datos de salud electrónicos. Los profesionales sanitarios deben abstenerse de obstaculizar la aplicación de los derechos de las personas físicas, como ocurriría si se negaran a tener en cuenta los datos de salud electrónicos personales procedentes de otro Estado miembro y que son proporcionados mediante el formato europeo de intercambio de historias clínicas electrónicas que es interoperable y fiable.

(16) El acceso a las historias clínicas electrónicas por parte de los prestadores de asistencia sanitaria u otras personas debe ser transparente para las personas físicas de que se trate. Los servicios de acceso a los datos de salud electrónicos deben proporcionar información pormenorizada sobre el acceso a los datos, por ejemplo, cuándo y qué entidad o persona física accedió a los datos y a qué datos se accedió. Las personas físicas también deben poder permitir o inhabilitar notificaciones automáticas relativas al acceso a los datos de salud electrónicos personales con los que guarden relación a través de los servicios de acceso de los profesionales sanitarios.

(17) Es posible que las personas físicas no deseen permitir el acceso a algunas partes de sus datos de salud electrónicos personales, aunque permitan el acceso a otras partes. Esto puede ser especialmente pertinente en casos de problemas de salud delicados, como los relacionados con la salud mental o sexual, procedimientos delicados como la interrupción voluntaria del embarazo, o datos sobre medicamentos específicos que puedan revelar otros problemas delicados. Por tanto, debe apoyarse este intercambio selectivo de datos de salud electrónicos personales y aplicarse mediante limitaciones establecidas por la persona física de que se trate de la misma manera dentro del territorio de un Estado miembro determinado como para el intercambio transfronterizo de datos. Esas limitaciones deben permitir una granularidad suficiente para limitar partes de los conjuntos de datos, como los elementos de las historias clínicas resumidas de los pacientes. Antes de establecer las limitaciones, se informará a las personas físicas de los riesgos para la seguridad del paciente asociados a la limitación del acceso a los datos de salud. Dado que la indisponibilidad de los datos de salud electrónicos personales restringidos puede afectar a la prestación o la calidad de los servicios sanitarios que reciba una persona física, las personas físicas que hagan uso de esas limitaciones deben

asumir la responsabilidad del hecho de que el prestador de asistencia sanitaria no pueda tener en cuenta los datos al prestar servicios sanitarios. Dichas limitaciones al acceso de datos de salud electrónicos personales pueden tener consecuencias que amenacen la vida y, por lo tanto, el acceso a esos datos debe ser posible, no obstante, cuando sea necesario para proteger intereses vitales en caso de emergencia. Los Estados miembros pueden establecer disposiciones jurídicas más específicas en su Derecho nacional sobre los mecanismos de limitación impuestos por las personas físicas a partes de sus datos de salud electrónicos personales, en particular en lo relativo a la responsabilidad médica en el caso de que la persona física de que se trate haya establecido esas limitaciones.

(18) Además, debido a las diferentes sensibilidades en los Estados miembros en lo que respecta al grado de control de los pacientes sobre sus datos de salud, los Estados miembros deben poder establecer un derecho absoluto de autoexclusión en relación con el acceso a sus datos de salud electrónicos personales por parte de cualquier persona distinta del responsable del tratamiento original, sin posibilidad de revocar esa autoexclusión en situaciones de emergencia. En tales casos, los Estados miembros deben establecer las reglas y salvaguardias específicas relativas a esos mecanismos de autoexclusión. Esas reglas y salvaguardias específicas también pueden referirse a categorías específicas de datos de salud electrónicos personales, por ejemplo, los datos genéticos. El derecho de autoexclusión significa que los datos de salud electrónicos personales relativos a la persona física que ejerce tal derecho no se pueden poner a disposición a través de los servicios creados en el marco del EEDS a otros que no sean el prestador de asistencia sanitaria que prescribió el tratamiento. Los Estados miembros deben poder exigir el registro y el almacenamiento de datos de salud electrónicos personales en un sistema HCE utilizado por el prestador de asistencia sanitaria que haya prestado los servicios sanitarios y a los que solo pueda acceder dicho prestador de asistencia sanitaria. Aunque una persona física haya ejercido ese derecho de autoexclusión, los prestadores de asistencia sanitaria van a seguir documentando el tratamiento dispensado de conformidad con las disposiciones aplicables y van a poder acceder a los datos registrados por ellos. Las personas físicas que ejerzan el derecho de autoexclusión deben poder revocar su decisión. En tales casos, los datos de salud electrónicos personales generados durante el período de autoexclusión podrían no estar disponibles a través de los servicios de acceso y MiSalud@UE.

(19) El acceso pleno y en tiempo oportuno de los profesionales sanitarios a las historias clínicas de los pacientes es fundamental para garantizar la continuidad de la asistencia, evitar duplicaciones y errores, y reducir costes. Sin embargo, debido a la falta de interoperabilidad, en muchos casos los profesionales sanitarios no pueden acceder a las historias clínicas completas de sus pacientes y no pueden tomar decisiones médicas óptimas para su diagnóstico y tratamiento, lo que añade costes considerables tanto para los sistemas sanitarios como para las personas físicas y puede dar lugar a peores resultados sanitarios para estas. Los datos de salud electrónicos disponibles en un formato interoperable y que puedan transmitirse entre los prestadores de asistencia sanitaria, también pueden reducir la carga administrativa que supone para los profesionales sanitarios introducir o copiar manualmente los datos de salud entre los sistemas electrónicos. Por consiguiente, para que los profesionales sanitarios utilicen datos de salud electrónicos personales en el ejercicio de sus funciones, deben disponer de los medios electrónicos adecuados, como dispositivos electrónicos y portales de profesionales sanitarios u otros servicios de acceso de los profesionales sanitarios. Dado que es difícil determinar exhaustivamente de antemano qué datos de los existentes en las categorías prioritarias son pertinentes desde el punto de vista médico en un acto concreto de asistencia, los profesionales sanitarios deben tener un amplio acceso a los datos. Al acceder a los datos relativos a sus pacientes, los profesionales sanitarios deben cumplir la normativa aplicable, los códigos de conducta, las directrices deontológicas u otras disposiciones que regulen la conducta ética con respecto al intercambio o el acceso a la información, en particular en situaciones que pongan en peligro la vida o en situaciones extremas. De conformidad con el Reglamento (UE) 2016/679, a fin de limitar su acceso a lo que sea pertinente en un acto concreto de asistencia, los prestadores de asistencia sanitaria deben seguir el principio de minimización de datos al acceder a los datos de salud electrónicos personales, limitando los datos a los que se acceda a aquellos datos que sean estrictamente necesarios y estén justificados para un servicio determinado. La prestación de servicios de acceso de los profesionales sanitarios es una misión asignada en interés público por el presente Reglamento y cuya realización requiere el tratamiento de datos personales en el sentido del artículo 6, apartado 1, letra e), del Reglamento (UE) 2016/679. El presente Reglamento establece condiciones y garantías para el tratamiento de datos de salud electrónicos en el servicio de acceso de los profesionales sanitarios de conformidad con el artículo 9, apartado 2, letra h), del Reglamento (UE) 2016/679, por ejemplo disposiciones pormenorizadas sobre el registro del acceso a datos de salud electrónicos personales y cuyo objetivo consiste en ofrecer transparencia a los interesados. No obstante, el presente Reglamento debe entenderse sin perjuicio del Derecho nacional relativo al tratamiento de datos de salud en la prestación de asistencia sanitaria, incluido el Derecho nacional que establezca las categorías de profesionales sanitarios que puedan tratar las diferentes categorías de datos de salud electrónicos.

(20) A fin de facilitar el ejercicio de los derechos complementarios de acceso y portabilidad establecidos en virtud del presente Reglamento, los Estados miembros deben establecer uno o varios servicios de acceso a datos de salud electrónicos. Esos servicios pueden prestarse a escala nacional, regional o local, o por prestadores de asistencia sanitaria, en forma de portal en línea para pacientes, aplicación para dispositivos móviles o por otros medios. Deben

concebirse de manera accesible, especialmente para las personas con discapacidad. Es de interés público esencial prestar un servicio de ese tipo, que permita a las personas físicas tener acceso fácilmente a sus datos de salud electrónicos personales. El tratamiento de datos de salud electrónicos personales a través de esos servicios es necesario para desempeñar la misión asignada por el presente Reglamento en el sentido del artículo 6, apartado 1, letra e), y del artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679. El presente Reglamento establece las condiciones y garantías necesarias para el tratamiento de los datos de salud electrónicos en los servicios de acceso a datos de salud electrónicos, como la identificación electrónica de las personas físicas que acceden a dichos servicios.

(21) Las personas físicas deben poder conceder una autorización a otras personas físicas de su elección, como a sus familiares u otras personas físicas cercanas, que permita a esas personas de su elección acceder a los datos de salud electrónicos personales de las personas físicas que conceden la autorización o controlar el acceso a ellos, o utilizar los servicios sanitarios digitales en su nombre. Esas autorizaciones también pueden ser convenientes para otras utilizaciones por parte de las personas físicas que dispongan de tales autorizaciones. Los Estados miembros, a fin de permitir y aplicar esas autorizaciones, deben establecer servicios de representación, que deben estar vinculados a servicios de acceso a datos de salud electrónicos personales, como son los portales de pacientes o las aplicaciones para dispositivos móviles orientadas al paciente. Esos servicios de representación también deben permitir a los tutores actuar en nombre de las personas a su cargo, incluidos los menores; en tales situaciones, las autorizaciones podrían ser automáticas. Además de esos servicios de representación, los Estados miembros también deben establecer servicios de apoyo fácilmente accesibles que sean prestados por personal adecuadamente formado, destinados a ayudar a las personas físicas en el ejercicio de sus derechos. A fin de tener en cuenta los casos en que mostrar algunos datos de salud electrónicos personales de las personas a su cargo a sus tutores pueda ser contraria a los intereses o la voluntad de las personas a su cargo, incluidos los menores, los Estados miembros deben poder establecer en el Derecho nacional limitaciones y garantías así como mecanismos para su aplicación técnica. Los servicios de acceso a los datos de salud electrónicos personales, como los portales de pacientes o las aplicaciones para dispositivos móviles orientadas al paciente, deben hacer uso de esas autorizaciones y permitir así que las personas físicas autorizadas accedan a los datos de salud electrónicos personales que entran en el ámbito de la autorización. Al objeto de aportar una solución horizontal con mayor facilidad de uso, las soluciones de representación digital deben adecuarse al Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([7]) y a las especificaciones técnicas de la cartera europea de identidad digital. Esa adecuación contribuiría a reducir las cargas administrativas y financieras de los Estados miembros mediante la atenuación del riesgo de desarrollar sistemas paralelos que no sean interoperables en toda la Unión.

(22) En algunos Estados miembros, la asistencia sanitaria la prestan equipos de gestión de la atención primaria, que son como grupos de profesionales sanitarios centrados en la atención primaria (como los médicos de familia), que realizan sus actividades de atención primaria sobre la base de un plan de asistencia sanitaria elaborado por ellos. En varios Estados miembros existen también otros tipos de equipos de asistencia sanitaria para otros fines asistenciales. En el contexto del uso primario en el EEDS, debe proporcionarse el acceso a los profesionales sanitarios pertenecientes a esos equipos.

(23) Las autoridades de control establecidas de conformidad con el Reglamento (UE) 2016/679 son competentes para supervisar y garantizar la aplicación de ese Reglamento, en particular para supervisar el tratamiento de los datos de salud electrónicos personales y para tramitar las reclamaciones presentadas por las personas físicas afectadas. El presente Reglamento establece derechos adicionales para las personas físicas en relación con el uso primario, que van más allá y complementan los derechos de acceso y portabilidad reconocidos en el Reglamento (UE) 2016/679. Debido a que estos derechos adicionales también deben ser protegidos por las autoridades de control establecidas de conformidad con el Reglamento (UE) 2016/679, los Estados miembros deben garantizar que esas autoridades de control dispongan de los recursos financieros y humanos, así como de los locales y las infraestructuras necesarios para el desempeño efectivo de esas funciones adicionales. La autoridad o autoridades de control responsables de la supervisión y la ejecución del tratamiento de datos de salud electrónicos personales para uso primario de conformidad con el presente Reglamento deben ser competentes para imponer multas administrativas. El ordenamiento jurídico de Dinamarca no permite las multas administrativas tal como se establecen en el presente Reglamento. Las disposiciones sobre multas administrativas pueden aplicarse de tal manera que en Dinamarca las multas sean impuestas por los órganos jurisdiccionales nacionales competentes como sanciones penales, siempre que tal aplicación de la normativa tenga un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En todo caso, las multas impuestas deben ser efectivas, proporcionadas y disuasorias.

([7]) Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

(24) Los Estados miembros deberían esforzarse por adherirse a principios éticos, como los principios éticos europeos para la salud digital adoptados por la red de sanidad electrónica el 26 de enero de 2022 y el principio de confidencialidad profesional entre los profesionales sanitarios y los pacientes, cuando apliquen el presente Reglamento. Reconociendo la importancia de los principios éticos, los principios éticos europeos para la salud digital proporcionan orientación a profesionales, investigadores, innovadores, responsables políticos y reguladores.

(25) La pertinencia de las diferentes categorías de datos de salud electrónicos para los distintos escenarios de asistencia sanitaria varía. Las diferentes categorías también han alcanzado distintos niveles de madurez respecto a la normalización, por lo que la aplicación de mecanismos para su intercambio puede ser más o menos compleja en función de la categoría. Por lo tanto, la mejora de la interoperabilidad y el intercambio de datos debe ser gradual y es necesario dar prioridad a ciertas categorías de datos de salud electrónicos. Entre las categorías de datos de salud electrónicos, la red de sanidad electrónica ha seleccionado las historias clínicas resumidas de los pacientes, las recetas y dispensaciones electrónicas, estudios de diagnóstico por imagen y los informes de imágenes correspondientes, los resultados de pruebas diagnósticas (como los resultados de laboratorio e informes correspondientes) y los informes de alta como los más pertinentes para la mayoría de las situaciones de asistencia sanitaria, y deben considerarse categorías prioritarias, en cuanto a la aplicación de su acceso y su transmisión, por parte de los Estados miembros. Cuando esas categorías de datos prioritarias representen grupos de datos de salud electrónicos, el presente Reglamento debe aplicarse tanto a los grupos en su totalidad como a las entradas de datos individuales que sean parte de esos grupos. Por ejemplo, dado que el estado de vacunación forma parte de una historia clínica resumida del paciente, los derechos y requisitos relacionados con la historia clínica resumida del paciente también deben aplicarse a esa situación de vacunación, aunque se trate por separado de la historia clínica resumida del paciente en su conjunto. Cuando se identifiquen nuevas necesidades de intercambio de categorías adicionales de datos de salud electrónicos a efectos de asistencia sanitaria, debe ser posible, en virtud del presente Reglamento, el acceso a esas categorías adicionales, y su intercambio. Las categorías adicionales deben aplicarse en primer lugar a escala de los Estados miembros y el presente Reglamento debe disponer el intercambio voluntario de dichas categorías de datos en situaciones transfronterizas entre los Estados miembros que cooperen. Debe prestarse especial atención al intercambio de datos en las regiones fronterizas de los Estados miembros vecinos en las que la prestación de servicios sanitarios transfronterizos es más frecuente y necesita procedimientos aún más rápidos que en toda la Unión en general.

(26) El nivel de disponibilidad de datos personales de salud y genéticos en formato electrónico varía de un Estado miembro a otro. El EEDS debe facilitar a las personas físicas la disponibilidad de esos datos en formato electrónico y un mejor control sobre el acceso y el intercambio de sus datos de salud electrónicos personales. Esto también contribuiría a la consecución del objetivo de que el 100 % de los ciudadanos de la Unión tengan acceso a sus historias clínicas electrónicas de aquí a 2030, tal como se menciona en la Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo ([8]). Con el fin de que los datos de salud electrónicos sean accesibles y transmisibles, el acceso a ellos y su transmisión deben poder realizarse en un formato europeo interoperable común de intercambio de historias clínicas electrónicas, al menos para determinadas categorías de datos de salud electrónicos, como las historias clínicas resumidas de los pacientes, las recetas y dispensaciones electrónicas, los estudios de diagnóstico por imagen y los informes de imágenes correspondientes, los resultados de pruebas diagnósticas y los informes de alta, respetando unos períodos transitorios. Cuando una persona física ponga datos de salud electrónicos personales a disposición de un prestador de asistencia sanitaria o una farmacia, o estos datos sean transmitidos por otro responsable del tratamiento en el formato europeo de intercambio de historias clínicas electrónicas, dicho formato debe ser aceptado y el destinatario debe ser capaz de leer los datos y usarlos para la prestación de asistencia sanitaria o para la dispensación de medicamentos, apoyando así la prestación de servicios sanitarios o la dispensación de la receta electrónica. El formato europeo de intercambio de historias clínicas electrónicas debería ser concebido de manera que facilite la traducción de los datos de salud electrónicos que se comuniquen mediante ese formato a las lenguas oficiales de la Unión, en la medida de lo posible. La Recomendación (UE) 2019/243 de la Comisión ([9]) sienta las bases de dicho formato europeo común de intercambio de historias clínicas electrónicas. La interoperabilidad del EEDS debería contribuir a unos conjuntos de datos de salud europeos de elevada calidad. El uso de un formato europeo de intercambio de historias clínicas electrónicas debería extenderse más en la Unión y en el plano nacional. El formato europeo de intercambio de historias clínicas electrónicas podría permitir diferentes perfiles para su utilización a escala de los sistemas HCE y de los puntos de contacto nacionales para la salud digital en MiSalud@UE para el intercambio transfronterizo de datos.

(27) Aunque los sistemas HCE están muy extendidos, el nivel de digitalización de los datos de salud varía en los Estados miembros en función de las categorías de datos y de la cobertura de los prestadores de asistencia sanitaria que registran datos de salud en formato electrónico. Es necesaria una acción de la Unión para apoyar la aplicación de los derechos de acceso a los datos de salud electrónicos por parte de los interesados y evitar así una mayor fragmentación. Con el fin de contribuir a una elevada calidad y a la continuidad de la asistencia sanitaria, determinadas categorías de datos de salud deben registrarse sistemáticamente en formato electrónico y con arreglo a requisitos específicos de calidad de los datos. El formato europeo de intercambio de historias clínicas electrónicas

([8]) Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030 (DO L 323 de 19.12.2022, p. 4).

([9]) Recomendación (UE) 2019/243 de la Comisión, de 6 de febrero de 2019, sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo (DO L 39 de 11.2.2019, p. 18).

debe constituir la base de las especificaciones relacionadas con el registro y el intercambio de datos de salud electrónicos.

(28) La telemedicina se está convirtiendo en una herramienta cada vez más importante que puede proporcionar a los pacientes acceso a la asistencia y hacer frente a las desigualdades. Tiene el potencial de reducir las desigualdades en materia de salud y reforzar la libre circulación transfronteriza de los ciudadanos de la Unión. Las herramientas digitales y otras herramientas tecnológicas pueden facilitar la prestación de asistencia en regiones remotas. Cuando los servicios digitales acompañen a la prestación física de un servicio de asistencia sanitaria, estos deben incluirse en la prestación general de asistencia. De conformidad con el artículo 168 del Tratado de Funcionamiento de la Unión Europea (TFUE), los Estados miembros son responsables de su política sanitaria, en particular de la organización y prestación de servicios sanitarios y atención médica, incluida la regulación de actividades como las farmacias en línea, la telemedicina y otros servicios que prestan y reembolsan, de conformidad con su legislación nacional. No obstante, las diferentes políticas de asistencia sanitaria no deben constituir obstáculos a la libre circulación de los datos de salud electrónicos en el contexto de la asistencia sanitaria transfronteriza, por ejemplo, la telemedicina y los servicios farmacéuticos en línea.

(29) El Reglamento (UE) n.º 910/2014 establece las condiciones en las que los Estados miembros efectúan la identificación de las personas físicas en situaciones transfronterizas utilizando medios de identificación expedidos por otro Estado miembro, con lo que se establecen disposiciones para el reconocimiento mutuo de dichos medios de identificación electrónica. El EEDS requiere un acceso seguro a los datos de salud electrónicos, también en situaciones transfronterizas. Los servicios de acceso a datos de salud electrónicos y los servicios de telemedicina deben permitir a las personas físicas ejercer sus derechos, independientemente de su Estado miembro de afiliación, y, por tanto, deben apoyar la identificación de las personas físicas que utilicen cualquier medio de identificación electrónica reconocido en virtud del Reglamento (UE) n.º 910/2014. Dadas las posibles dificultades en la correspondencia de la identidad en situaciones transfronterizas, podría ser necesario que los Estados miembros de tratamiento tengan que proporcionar mecanismos de acceso complementarios, como fichas o códigos, a las personas físicas que llegan de otros Estados miembros y reciben asistencia sanitaria. La Comisión debe estar facultada para adoptar actos de ejecución para determinar los requisitos de la identificación y autenticación interoperables y transfronterizas de las personas físicas y los profesionales sanitarios, incluido todo mecanismo complementario que sea necesario para garantizar que las personas físicas puedan ejercer sus derechos relacionados con los datos de salud electrónicos personales en situaciones transfronterizas.

(30) Los Estados miembros deben designar autoridades de salud digital pertinentes para la planificación y aplicación de normas de acceso a los datos de salud electrónicos, su transmisión y la garantía del respeto de los derechos de las personas físicas y los profesionales sanitarios, en forma de autoridades independientes o como parte de las autoridades ya existentes. El personal de la autoridad de salud digital no debe tener ningún interés económico ni de otro tipo en empresas o actividades económicas que puedan comprometer su imparcialidad. En la mayoría de los Estados miembros ya existen autoridades de salud digital que se ocupan de los HCE, la interoperabilidad, la seguridad o la normalización. Cuando desempeñen sus funciones, las autoridades de salud digital deben cooperar, en particular, con las autoridades de control establecidas en virtud del Reglamento (UE) 2016/679 y los organismos de supervisión establecidos en virtud del Reglamento (UE) n.º 910/2014. Las autoridades de salud digital también pueden cooperar con el Consejo Europeo de Inteligencia Artificial creado por el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo ([10]), el Grupo de Coordinación de Productos Sanitarios creado por el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo ([11]), el Comité Europeo de Innovación en materia de Datos creado en virtud del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo ([12]) y las autoridades competentes en virtud del Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo ([13]). Los Estados miembros deben facilitar la participación de los agentes nacionales en la cooperación a escala de la Unión, la canalización de los conocimientos especializados y el asesoramiento sobre el diseño de las soluciones necesarias para alcanzar los objetivos del EEDS.

([10]) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689 de 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([11]) Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1).

([12]) Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) (DO L 152 de 3.6.2022, p. 1).

([13]) Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (DO L, 2023/2854 de 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(31) Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica debe tener derecho a la tutela judicial efectiva contra decisiones jurídicamente vinculantes de autoridades de salud digital que les concierna o en caso de que la autoridad de salud digital no dé curso a una reclamación o no informe a la persona física o jurídica en el plazo de tres meses sobre el curso o el resultado de la reclamación. Toda acción contra una autoridad de salud digital se ejercitará ante los órganos jurisdiccionales del Estado miembro en el que dicha autoridad esté establecida.

(32) Las autoridades de salud digital deben contar con suficientes capacidades técnicas, tal vez reuniendo a expertos de diferentes organizaciones. Las actividades de las autoridades de salud digital deben planificarse y supervisarse adecuadamente para garantizar su eficiencia. Las autoridades de salud digital deben adoptar las medidas necesarias para proteger los derechos de las personas físicas mediante la creación de soluciones técnicas nacionales, regionales y locales, como las soluciones nacionales de intermediación de HCE y los portales de pacientes. Al adoptar tales medidas de protección necesarias, las autoridades de salud digital deben aplicar normas y especificaciones comunes a dichas soluciones, promover la aplicación de las normas y especificaciones en los procedimientos de contratación y utilizar otros medios innovadores, incluido el reembolso de soluciones que cumplan los requisitos de interoperabilidad y seguridad del EEDS. Los Estados miembros deben garantizar que se imparten iniciativas de formación adecuadas. En particular, los profesionales sanitarios deben recibir información y formación sobre sus derechos y obligaciones en virtud del presente Reglamento. Para desempeñar sus funciones, las autoridades de salud digital deben cooperar a nivel de la Unión y nacional con otras entidades, incluidos los organismos de seguros, los prestadores de asistencia sanitaria, los profesionales sanitarios, los fabricantes de sistemas HCE y de aplicaciones de bienestar, así como otras partes interesadas del sector de la salud o de las tecnologías de la información, las entidades que gestionan los regímenes de reembolso, los organismos de evaluación de tecnologías sanitarias, las autoridades y agencias reguladoras de medicamentos, las autoridades de productos sanitarios, los compradores y las autoridades de ciberseguridad o identificación electrónica.

(33) El acceso a los datos de salud electrónicos y su transmisión son pertinentes en situaciones de asistencia sanitaria transfronteriza, ya que pueden contribuir a la continuidad de la asistencia sanitaria cuando las personas físicas viajan a otros Estados miembros o cambian de lugar de residencia. La continuidad de la asistencia y el acceso rápido a los datos de salud electrónicos personales son aún más importantes para los residentes en las regiones fronterizas, que cruzan la frontera con frecuencia para recibir asistencia sanitaria. En muchas regiones fronterizas, algunos servicios sanitarios especializados pueden estar más cerca al otro lado de la frontera que en el mismo Estado miembro. La transmisión transfronteriza de datos de salud electrónicos personales en situaciones en las que una persona física está utilizando servicios de un prestador de asistencia sanitaria establecido en otro Estado miembro necesita una infraestructura. Debe considerarse la ampliación gradual de esa infraestructura y su financiación. A tal efecto, se ha creado una infraestructura voluntaria, MiSalud@UE (*MyHealth@EU*), como parte de las acciones previstas para alcanzar los objetivos marcados en la Directiva 2011/24/UE del Parlamento Europeo y del Consejo ([14]). A través de MiSalud@UE, los Estados miembros empezaron a ofrecer a las personas físicas la posibilidad de compartir sus datos de salud electrónicos personales con los prestadores de asistencia sanitaria cuando viajan al extranjero. Sobre la base de esa experiencia, la participación de los Estados miembros en MiSalud@UE, con arreglo a lo previsto en el presente Reglamento, debe ser obligatoria. Las especificaciones técnicas de MiSalud@UE deben permitir el intercambio de categorías prioritarias de datos de salud electrónicos, así como categorías adicionales incluidas en el formato europeo de intercambio de historias clínicas electrónicas. Esas especificaciones deben definirse mediante actos de ejecución y basarse en las especificaciones transfronterizas del formato europeo de intercambio de historias clínicas electrónicas, complementadas con especificaciones adicionales sobre ciberseguridad, interoperabilidad técnica y semántica, operaciones y gestión de servicios. Debe exigirse a los Estados miembros que se unan a MiSalud@UE, cumplan sus especificaciones técnicas, y conecten a ella a los prestadores de asistencia sanitaria, incluidas las farmacias, ya que es algo necesario para permitir a las personas físicas ejercer su derecho en el marco del presente Reglamento a acceder a sus datos de salud electrónicos personales y su derecho a hacer uso de dichos datos independientemente del Estado miembro en el que la persona física se encuentre.

(34) MiSalud@UE proporciona una infraestructura común a los Estados miembros para garantizar la conectividad y la interoperabilidad de manera eficiente y segura para apoyar la asistencia sanitaria transfronteriza, sin que ello afecte a las responsabilidades de los Estados miembros antes y después de la transmisión de los datos de salud electrónicos personales a través de ella. Los Estados miembros son responsables de la organización de sus puntos de contacto nacionales para la salud digital y del tratamiento de datos personales a efectos de la prestación de asistencia sanitaria antes y después de la transmisión de dichos datos a través de MiSalud@UE. La Comisión debe realizar un seguimiento, mediante comprobaciones del cumplimiento, sobre si los puntos de contacto nacionales para la salud digital cumplen los requisitos necesarios con respecto al desarrollo técnico de MiSalud@UE y las reglas pormenorizadas relativas a la seguridad, la confidencialidad y la protección de los datos de salud electrónicos personales. En caso de incumplimiento grave por parte de un punto de contacto nacional para la salud digital, la Comisión debe poder suspender los servicios afectados por el incumplimiento prestados por ese punto de contacto nacional para la salud digital. La Comisión debe actuar como encargada del tratamiento en nombre de los Estados

([14]) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

miembros dentro de MiSalud@UE y debe prestar servicios centrales para ella. A fin de garantizar el cumplimiento de la normativa sobre protección de datos y proporcionar un marco de gestión de riesgos para la transmisión de datos de salud electrónicos personales, las responsabilidades específicas de los Estados miembros, como corresponsables del tratamiento, y las obligaciones de la Comisión como encargada del tratamiento en su nombre deben detallarse mediante actos de ejecución. Cada Estado miembro es el único responsable de los datos y servicios en dicho Estado miembro. El presente Reglamento constituye la base jurídica para el tratamiento de datos de salud electrónicos personales en MiSalud@UE como misión realizada en interés público asignada por el Derecho de la Unión a que se refiere el artículo 6, apartado 1, letra e), del Reglamento (UE) 2016/679. Ese tratamiento es necesario para la prestación de asistencia sanitaria en situaciones transfronterizas, tal como se menciona en el artículo 9, apartado 2, letra h), de dicho Reglamento.

(35) Además de los servicios de MiSalud@UE para el intercambio de datos de salud electrónicos personales basados en el formato europeo de intercambio de historias clínicas electrónicas, pueden ser necesarios otros servicios o infraestructuras complementarias, por ejemplo en casos de emergencias de salud pública o cuando la arquitectura de MiSalud@UE no sea adecuada para la aplicación de algunos casos de uso. Algunos ejemplos de tales casos de uso son el apoyo a las funcionalidades de la tarjeta de vacunación, incluido el intercambio de información sobre los planes de vacunación, o la verificación de los certificados de vacunación o de otros certificados relacionados con la salud. Esos casos de uso adicionales podrían ser importantes para introducir una funcionalidad adicional para gestionar las crisis sanitarias, como el apoyo al rastreo de contactos con el fin de contener la propagación de enfermedades infecciosas. MiSalud@UE debe posibilitar los intercambios de datos de salud electrónicos personales con los puntos de contacto nacionales para la salud digital de los terceros países y los sistemas pertinentes establecidos a nivel internacional por organizaciones internacionales para contribuir a la continuidad de la asistencia sanitaria. Esto es especialmente importante para los particulares que viajan a terceros países vecinos o desde ellos, los países candidatos y los países y territorios de ultramar asociados. Se debe comprobar la conexión de esos puntos de contacto nacionales para la salud digital de terceros países a MiSalud@UE y la interoperabilidad con los sistemas digitales establecidos a nivel internacional por organizaciones internacionales, para garantizar que dichos puntos de contacto y sistemas digitales cumplan las especificaciones técnicas, la normativa sobre protección de datos y otros requisitos de MiSalud@UE. Además, dado que la conexión a MiSalud@UE va a implicar transferencias a terceros países de datos de salud electrónicos personales, como el hecho de compartir la historia clínica resumida del paciente cuando este solicite asistencia en ese tercer país, será necesaria la puesta en marcha de los instrumentos de transferencia pertinentes de conformidad con el capítulo V del Reglamento (UE) 2016/679. La Comisión debe estar facultada para adoptar actos de ejecución a fin de facilitar la conexión a MiSalud@UE de esos puntos de contacto nacionales para la salud digital de terceros países y sistemas establecidos a nivel internacional por organizaciones internacionales. Al preparar esos actos de ejecución, la Comisión debe tener en cuenta los intereses de seguridad nacional de los Estados miembros.

(36) A fin de permitir el intercambio fluido de los datos de salud electrónicos y garantizar el respeto de los derechos de las personas físicas y los profesionales sanitarios, los sistemas HCE comercializados en el mercado interior deben poder almacenar y transmitir, de manera segura, datos de salud electrónicos de elevada calidad. Este es un objetivo clave del EEDS para garantizar la seguridad y la libre circulación de los datos de salud electrónicos en toda la Unión. A tal fin, debe establecerse un régimen de autoevaluación de la conformidad obligatoria para los sistemas HCE que traten datos de salud electrónicos de una o más categorías prioritarias, superando así la fragmentación del mercado al mismo tiempo que se garantiza un enfoque proporcionado. Mediante la autoevaluación, los sistemas HCE van a demostrar el cumplimiento de los requisitos en materia de interoperabilidad, seguridad y registro para la comunicación de datos de salud electrónicos personales establecidos por los dos componentes obligatorios de programa informático para HCE armonizados por el presente Reglamento, a saber, el componente de programa informático europeo de interoperabilidad para sistemas HCE y el componente de programa informático europeo de registro para sistemas HCE (en lo sucesivo, «componentes armonizados de programa informático de sistemas HCE»). Los componentes armonizados de programa informático de sistemas HCE se refieren principalmente a la transformación de los datos, aunque pueden implicar la necesidad de requisitos indirectos para el registro y la presentación de datos en los sistemas HCE. Las especificaciones técnicas para los componentes armonizados de programa informático de sistemas HCE deben determinarse mediante actos de ejecución y basarse en el uso del formato europeo de intercambio de historias clínicas electrónicas. Los componentes armonizados de programa informático de sistemas HCE deben concebirse para ser reutilizables e integrarse sin problema con otros componentes dentro de un sistema de programa lógico más amplio.Los requisitos de seguridad de los componentes armonizados de programa informático de sistemas HCE deben incluir elementos específicos de los sistemas HCE, ya que las propiedades de seguridad más generales deben estar incluidas en otros mecanismos, como los del Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo ([15]). Para apoyar ese proceso, deben crearse entornos digitales europeos de pruebas para proporcionar medios automatizados para comprobar si el funcionamiento de los componentes armonizados de programa informático de un sistema HCE cumple con los

([15]) Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE)n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) (DO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

requisitos establecidos en el presente Reglamento. A tal fin, deben conferirse a la Comisión competencias de ejecución para determinar las especificaciones comunes para esos entornos. La Comisión debe desarrollar los programas informáticos necesarios para los entornos de pruebas y ponerlos a disposición como fuente abierta. Debe corresponder a los Estados miembros la gestión de los entornos digitales de pruebas, ya que están más cerca de los fabricantes y mejor situados para apoyarlos. Los fabricantes deben utilizar esos entornos digitales de pruebas para probar sus productos antes de introducirlos en el mercado, al mismo tiempo que siguen siendo plenamente responsables de la conformidad de sus productos. Los resultados de las pruebas deben formar parte de la documentación técnica del producto. Cuando el sistema HCE o cualquier parte del mismo cumpla las normas europeas o las especificaciones comunes, también se indicará la lista de las normas europeas y las especificaciones comunes pertinentes en la documentación técnica. Para apoyar la comparabilidad de sistemas HCE, la Comisión debe preparar una plantilla uniforme para la documentación técnica que acompañe dichos sistemas.

(37) Los sistemas HCE deben ir acompañados de una ficha informativa que incluya información para sus usuarios profesionales y de instrucciones de uso claras y completas, también en un formato accesible para personas con discapacidad. Si un sistema HCE no va acompañado de esa información, se debe exigir al fabricante del sistema HCE de que se trate, a su representante autorizado y a todos los demás operadores económicos pertinentes que añadan al sistema HCE esa ficha informativa e instrucciones de uso.

(38) Si bien los sistemas HCE destinados específicamente por el fabricante a ser utilizados para el tratamiento de una o más categorías específicas de datos de salud electrónicos deben estar sometidos a una autocertificación obligatoria, los programas informáticos para fines generales no deben considerarse sistemas HCE, ni siquiera cuando se utilicen en un contexto de asistencia sanitaria, y, por tanto, no se debe exigir que cumplan lo dispuesto en el presente Reglamento. Esto incluye casos como los programas informáticos de tratamiento de texto utilizados para redactar informes que pasarían a formar parte de las historias clínicas electrónicas escritas, de la plataforma de uso general o del programa informático de gestión de bases de datos que se utilice como parte de las soluciones de almacenamiento de datos.

(39) El presente Reglamento impone un régimen de autoevaluación de la conformidad obligatoria para los componentes de programa informático armonizados de sistemas HCE, a fin de garantizar que los sistemas HCE introducidos en el mercado de la Unión puedan intercambiar datos en el formato europeo de intercambio de historias clínicas electrónicas y que dispongan de las capacidades de registro necesarias. Dicha autoevaluación de la conformidad obligatoria, que toma forma de declaración UE de conformidad del fabricante, debe garantizar que esos requisitos se cumplan de manera proporcionada, al mismo tiempo que se evite una carga indebida para los Estados miembros y los fabricantes.

(40) Los fabricantes deben colocar en los documentos que acompañen al sistema HCE y, en su caso en el envase, un marcado CE de conformidad que indique que el sistema HCE cumple con el presente Reglamento y, con respecto a los aspectos no regulados por el presente Reglamento, con otra normativa de la Unión aplicable que también exija la colocación de tal marcado. Los Estados miembros deben basarse en los mecanismos existentes para garantizar la correcta aplicación de las disposiciones sobre el marcado CE de conformidad de la normativa de la Unión pertinente y deben adoptar las medidas adecuadas en caso de un uso indebido de ese marcado.

(41) Los Estados miembros deben seguir siendo competentes para determinar los requisitos relativos a cualquier otro componente de programa informático de sistemas HCE, así como las condiciones generales para la conexión de los prestadores de asistencia sanitaria a sus respectivas infraestructuras nacionales, que pueden ser objeto de evaluación por terceros a nivel nacional. A fin de facilitar el buen funcionamiento del mercado interior de los sistemas de HCE, los productos sanitarios digitales y los servicios asociados, es necesario garantizar tanto como sea posible la transparencia en lo que respecta al Derecho nacional que establece requisitos para los sistemas HCE y a las disposiciones sobre su evaluación de la conformidad en relación con aspectos distintos de los componentes armonizados de programa informático de sistemas HCE. Por lo tanto, los Estados miembros deben informar a la Comisión de esos requisitos nacionales para que disponga de la información necesaria para garantizar que no afectan negativamente a los componentes armonizados de programa informático de sistemas HCE.

(42) Ciertos componentes de programa informático de sistemas HCE podrían considerarse productos sanitarios con arreglo al Reglamento (UE) 2017/745 o productos sanitarios para diagnóstico *in vitro* con arreglo al Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo ([16]). Los programas informáticos o los módulos de estos que entren en la definición de producto sanitario, productos sanitarios para diagnóstico *in vitro* o de un sistema de inteligencia artificial (IA) considerado de alto riesgo (en lo sucesivo, «sistema de IA de alto riesgo») deben estar certificados de conformidad con los Reglamentos (UE) 2017/745, (UE) 2017/746 y (UE) 2024/1689, según proceda. Si bien esos productos han de cumplir obligatoriamente los requisitos previstos en los Reglamentos respectivos que los rigen, los Estados miembros deben adoptar las medidas adecuadas para garantizar que la evaluación de la conformidad correspondiente se efectúe como un procedimiento conjunto o coordinado, a fin de limitar la carga administrativa de los fabricantes y otros operadores económicos. Los requisitos esenciales de interoperabilidad del presente Reglamento solo deben aplicarse en la medida en que el fabricante de un producto sanitario, de un producto sanitario para diagnóstico *in vitro* o de un sistema de IA de alto riesgo que proporcione datos de salud electrónicos

([16]) Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión (DO L 117 de 5.5.2017, p. 176).

que vayan a ser tratados como parte del sistema HCE, alegue interoperabilidad con dicho sistema. En tal caso, las disposiciones sobre especificaciones comunes para los sistemas HCE deben ser aplicables a dichos productos sanitarios, productos sanitarios para diagnóstico *in vitro* y sistemas de IA de alto riesgo.

(43) Para apoyar aún más la interoperabilidad y la seguridad, los Estados miembros deben poder mantener o determinar reglas específicas para la adquisición, el reembolso o la financiación de sistemas HCE a nivel nacional en el contexto de la organización, la prestación o la financiación de los servicios sanitarios. Dichas reglas específicas no deben obstaculizar la libre circulación de los sistemas HCE en la Unión. Algunos Estados miembros han introducido la certificación obligatoria de los sistemas HCE o las pruebas de interoperabilidad obligatorias para su conexión a los servicios sanitarios digitales nacionales. Esos requisitos suelen reflejarse en los procedimientos de contratación organizados por los prestadores de asistencia sanitaria y las autoridades nacionales o regionales. La certificación obligatoria de los sistemas HCE a escala de la Unión debe establecer una base de referencia que pueda utilizarse en los procedimientos de contratación a nivel nacional.

(44) A fin de garantizar el ejercicio efectivo por parte de los pacientes de sus derechos en virtud del presente Reglamento, los prestadores de asistencia sanitaria que desarrollen y utilicen un sistema HCE interno para realizar actividades internas sin introducirlo en el mercado a cambio de un pago o remuneración, también deben cumplir lo dispuesto en el presente Reglamento. En este contexto, dichos prestadores de asistencia sanitaria deben cumplir todos los requisitos aplicables a los fabricantes respecto de tales sistemas HCE que son desarrollados internamente y que dichos prestadores de asistencia sanitaria han puesto en servicio. Sin embargo, dado que los prestadores de asistencia sanitaria pueden necesitar más tiempo para prepararse a fin de cumplir el presente Reglamento, esos requisitos solo deben aplicarse a dichos sistemas tras un período transitorio ampliado.

(45) Es necesario establecer una división clara y proporcionada de las obligaciones que se corresponden con la función de cada operador económico en el proceso de suministro y distribución de los sistemas HCE. Los operadores económicos deben ser responsables de cumplir sus respectivas funciones en dicho proceso y garantizar que solo se comercialicen sistemas HCE que cumplan los requisitos pertinentes.

(46) Los fabricantes de sistemas HCE deben demostrar el cumplimiento de los requisitos esenciales en materia de interoperabilidad y seguridad mediante la aplicación de especificaciones comunes. A tal fin, deben conferirse a la Comisión competencias de ejecución para determinar dichas especificaciones comunes relativas a los conjuntos de datos, los sistemas de codificación, las especificaciones técnicas, normas, especificaciones y perfiles para el intercambio de datos, así como los requisitos y principios relacionados con la seguridad de los pacientes y la seguridad, la confidencialidad, la integridad y la protección de los datos personales, y las especificaciones y requisitos relacionados con la gestión de la identificación y el uso de la identificación electrónica. Las autoridades de salud digital deben contribuir al desarrollo de dichas especificaciones comunes. Cuando proceda, esas especificaciones comunes deben basarse en las normas armonizadas existentes para los componentes armonizados de programa informático de sistemas HCE y ser compatibles con el Derecho sectorial. Cuando las especificaciones comunes tengan una importancia particular en relación con los requisitos de protección de datos personales de los sistemas HCE, se someterán a consulta con el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) antes de su adopción, de conformidad con el artículo 42, apartado 2, del Reglamento (UE) 2018/1725.

(47) Con el objetivo de garantizar el cumplimiento adecuado y efectivo de los requisitos y las obligaciones previstos en el presente Reglamento, debe aplicarse el sistema relativo a la vigilancia del mercado y la conformidad de los productos establecido por el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo ([17]). Dependiendo de la organización definida a nivel nacional, dichas actividades de vigilancia del mercado podrían ser llevadas a cabo por las autoridades de salud digital que garanticen la correcta aplicación del capítulo II del presente Reglamento o por una autoridad de vigilancia del mercado independiente responsable de los sistemas HCE. Si bien la designación de autoridades de salud digital como autoridades de vigilancia del mercado podría tener importantes ventajas prácticas para proporcionar la asistencia sanitaria y la asistencia, debe evitarse cualquier conflicto de intereses, por ejemplo separando diferentes funciones.

(48) El personal de las autoridades de vigilancia del mercado no debe tener ningún conflicto de intereses económico, financiero o personal, directo ni indirecto, que pueda considerarse perjudicial para su independencia y, en particular, no se deben encontrar en una situación que pueda afectar directa o indirectamente a la imparcialidad de su conducta profesional. Los Estados miembros deben determinar y publicar el procedimiento de selección de las autoridades de vigilancia del mercado. Han de velar por que el procedimiento sea transparente y no permita conflictos de intereses.

(49) Los usuarios de aplicaciones de bienestar, incluidas las aplicaciones para dispositivos móviles, deben ser informados de la capacidad de dichas aplicaciones para conectarse y suministrar datos a los sistemas HCE o a las soluciones sanitarias electrónicas nacionales, en los casos en que los datos producidos por las aplicaciones de bienestar sean útiles para la asistencia sanitaria. La capacidad de esas aplicaciones para exportar datos en un formato interoperable

([17]) Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) n.º 305/2011 (DO L 169 de 25.6.2019, p. 1).

también es pertinente a efectos de la portabilidad de los datos. Cuando proceda, también debe informarse a los usuarios sobre el cumplimiento por parte de dichas aplicaciones de bienestar de los requisitos de interoperabilidad y seguridad. Sin embargo, dado el gran número de aplicaciones de bienestar y la escasa pertinencia de los datos producidos por muchas de ellas para la asistencia sanitaria, un régimen de certificación para esas aplicaciones no sería proporcionado. Por consiguiente, debe establecerse un régimen de etiquetado obligatorio para las aplicaciones de bienestar para las que se declare su interoperabilidad con los sistemas HCE como mecanismo adecuado para aportar transparencia para los usuarios de las aplicaciones de bienestar en lo que respecta al cumplimiento por estas de los requisitos en el marco del presente Reglamento, lo que debería ser de ayuda para los usuarios a la hora de elegir aplicaciones de bienestar adecuadas y con elevados niveles de interoperabilidad y seguridad. La Comisión debe establecer mediante actos de ejecución los detalles relativos al formato y el contenido de dicha etiqueta.

(50) Los Estados miembros deben seguir pudiendo regular libremente otros aspectos del uso de las aplicaciones de bienestar, siempre que las correspondientes reglas cumplan el Derecho de la Unión.

(51) La distribución de información sobre los sistemas HCE certificados y las aplicaciones de bienestar etiquetadas es necesaria para que los compradores y los usuarios de dichos productos puedan encontrar soluciones interoperables para sus necesidades específicas. Por consiguiente, debe crearse a escala de la Unión una base de datos de sistemas HCE interoperables y aplicaciones de bienestar, que no entren en el ámbito de aplicación de los Reglamentos (UE) 2017/745 y (UE) 2024/1689, similar a la base de datos europea sobre productos sanitarios (Eudamed) establecida por el Reglamento (UE) 2017/745. Los objetivos de la base de datos de la UE para el registro de sistemas HCE y aplicaciones de bienestar deben ser aumentar la transparencia general, evitar múltiples requisitos de notificación y racionalizar y facilitar el flujo de información. En el caso de los productos sanitarios y los sistemas de IA, el registro debe mantenerse en las bases de datos existentes establecidas, respectivamente, en virtud de los Reglamentos (UE) 2017/745 y (UE) 2024/1689, pero los fabricantes deben indicar el cumplimiento de los requisitos de interoperabilidad cuando lo declaren, a fin de proporcionar información a los compradores.

(52) Sin obstaculizar ni sustituir los acuerdos contractuales u otro tipo de mecanismo existente, el presente Reglamento tiene por objeto establecer un mecanismo común para acceder a los datos de salud electrónicos para uso secundario en toda la Unión. En el marco de ese mecanismo, los tenedores de datos de salud deben poner a disposición, sobre la base de un permiso de datos o de una petición de datos de salud, los datos que estén en su poder. Para el objetivo del tratamiento de datos de salud electrónicos para uso secundario, es necesaria una de las bases jurídicas a que se refiere el artículo 6, apartado 1, letras a), c), e) o f), del Reglamento (UE) 2016/679, conjuntamente con el artículo 9, apartado 2, de dicho Reglamento. En consecuencia, el presente Reglamento constituye una base jurídica para el uso secundario de datos de salud electrónicos personales incluidas las garantías exigidas según el artículo 9, apartado 2, letras g) a j), del Reglamento (UE) 2016/679 para permitir el tratamiento de categorías especiales de datos, en cuanto a la licitud de los fines, la fiabilidad de la gobernanza para proporcionar el acceso a los datos de salud, a través de la implicación de los organismos de acceso a datos de salud, y el tratamiento en un entorno de tratamiento seguro, así como disposiciones para el tratamiento de datos, establecidas en el permiso de datos. Por consiguiente, los Estados miembros ya no pueden mantener o introducir, en virtud del artículo 9, apartado 4, del Reglamento (UE) 2016/679, condiciones adicionales, incluidas limitaciones y disposiciones específicas que soliciten el consentimiento de las personas físicas, en relación con el tratamiento para uso secundario de datos de salud electrónicos personales en virtud del presente Reglamento, a excepción de la introducción de medidas más estrictas y salvaguardias adicionales a nivel nacional destinadas a salvaguardar la sensibilidad y el valor de determinados datos tal y como se dispone en el presente Reglamento. Los solicitantes de datos de salud también deben demostrar la existencia de una base jurídica a que se refiere el artículo 6 del Reglamento (UE) 2016/679 que les permita pedir el acceso a los datos de salud electrónicos de conformidad con el presente Reglamento y deben cumplir las condiciones establecidas en el capítulo IV del presente Reglamento.Además, el organismo de acceso a datos de salud debe valorar la información proporcionada por el solicitante de datos de salud, sobre la base de la cual debe poder expedir un permiso de datos para el tratamiento de datos de salud electrónicos personales con arreglo al presente Reglamento, que debe cumplir los requisitos establecidos en el capítulo IV del presente Reglamento. Para el tratamiento de datos de salud electrónicos en poder de los tenedores de datos de salud, el presente Reglamento crea la obligación jurídica, en el sentido del artículo 6, apartado 1, letra c), del Reglamento (UE) 2016/679, de conformidad con su artículo 9, apartado 2, letras i) y j), para el tenedor de datos de salud de poner a disposición de los organismos de acceso a datos de salud los datos de salud electrónicos personales, sin que se vea afectada la base jurídica a efectos del tratamiento inicial, por ejemplo, la prestación de asistencia sanitaria. El presente Reglamento también asigna misiones de interés público en el sentido del artículo 6, apartado 1, letra e), del Reglamento (UE) 2016/679 a los organismos de acceso a datos de salud, y cumple los requisitos del artículo 9, apartado 2, letras g) a j), según proceda, de dicho Reglamento. Si el usuario de datos de salud invoca la base jurídica establecida en el artículo 6, apartado 1, letra e) o f), del Reglamento (UE) 2016/679, el presente Reglamento debe establecer las garantías exigidas en virtud del artículo 9, apartado 2, del Reglamento (UE) 2016/679.

(53) Los datos de salud electrónicos utilizados para uso secundario pueden aportar beneficios sociales. Debe fomentarse la utilización de datos de la vida real y datos acreditativos de la vida real, incluidos resultados comunicados por los pacientes, a efectos de regulación y de formulación de políticas basándose en datos contrastados, así como para la investigación, la evaluación de tecnologías sanitarias y objetivos clínicos. Los datos de la vida real y los datos acreditativos de la vida real tienen el potencial para complementar los datos de salud actualmente disponibles. Para alcanzar ese objetivo, es importante que los conjuntos de datos puestos a disposición para uso secundario de conformidad con el presente Reglamento sean lo más completos posible. El presente Reglamento establece las garantías necesarias para atenuar determinados riesgos inherentes a la consecución de esos beneficios. El uso secundario de datos de salud electrónicos se basa en datos seudonimizados o anonimizados, con el fin de impedir la identificación de los interesados.

(54) Para equilibrar la necesidad de los usuarios de datos de salud de disponer de conjuntos de datos completos y representativos con la necesidad de autonomía de las personas físicas con respecto a sus datos de salud electrónicos personales que se consideren especialmente sensibles, las personas físicas deben poder decidir si sus datos de salud electrónicos personales pueden ser tratados para uso secundario en virtud del presente Reglamento, en forma de un derecho de autoexclusión a que esos datos se pongan a disposición para un uso secundario. Debe preverse un mecanismo para ejercer ese derecho de autoexclusión que sea fácilmente comprensible y accesible y de fácil utilización. Además, es indispensable proporcionar a las personas físicas información suficiente y completa sobre su derecho de autoexclusión, incluidos los beneficios e inconvenientes que conlleve el ejercicio de ese derecho. No debe exigirse a las personas físicas que expliquen los motivos de la autoexclusión y deben tener la posibilidad de reconsiderar su elección en cualquier momento. Sin embargo, para determinados fines con un fuerte vínculo con el interés público, como las actividades de protección contra las amenazas transfronterizas graves para la salud o la investigación científica por razones importantes de interés público, conviene prever la posibilidad de que los Estados miembros establezcan, teniendo en cuenta su contexto nacional, mecanismos para proporcionar acceso a los datos de salud electrónicos personales de las personas físicas que hayan ejercido su derecho de autoexclusión, a fin de garantizar que puedan ponerse a disposición conjuntos de datos completos en esas situaciones. Ese tipo de mecanismos deben cumplir los requisitos establecidos para el uso secundario en virtud del presente Reglamento. La investigación científica por razones importantes de interés público podría incluir, por ejemplo, la investigación que aborde necesidades médicas no satisfechas, incluidas las enfermedades raras o las amenazas emergentes para la salud. Las disposiciones sobre esas excepciones deben respetar la esencia de los derechos y libertades fundamentales y han de ser una medida necesaria y proporcionada en una sociedad democrática para satisfacer el interés público en relación con objetivos científicos y sociales legítimos.Esas excepciones solo deben estar disponibles para los usuarios de datos de salud que sean organismos del sector público, o instituciones, órganos u organismos de la Unión pertinentes con mandato para desempeñar una misión en el ámbito de la salud pública, u otra entidad a la que se haya encomendado el desempeño de una misión pública en el ámbito de la salud pública, o que actúe en nombre o por encargo de una autoridad pública, y solo cuando los datos no puedan ser obtenidos por medios alternativos de manera oportuna y eficaz. Esos usuarios de datos de salud deben justificar que el uso de la excepción es necesario para una solicitud de acceso individual a datos de salud o una petición de datos de salud. Cuando se aplique esa excepción, los usuarios de datos de salud deben seguir aplicando las garantías del capítulo IV, en particular la prohibición de reidentificación o de intentar reidentificar a las personas físicas afectadas.

(55) En el contexto del EEDS, los datos de salud electrónicos ya existen y están siendo recogidos por, entre otros, los prestadores de asistencia sanitaria, las asociaciones profesionales, las instituciones públicas, los reguladores, los investigadores y las aseguradoras en el curso de sus actividades. Aunque esos datos también deben estar disponibles para uso secundario, a saber, para el tratamiento de datos con fines distintos de aquellos para los que se recogieron o produjeron, muchos de ellos no se ponen a disposición para el tratamiento con esos otros fines. Esto limita la capacidad de investigadores, innovadores, responsables políticos, reguladores y médicos para utilizar esos datos con diferentes fines, como la investigación, la innovación, la formulación de políticas, la regulación, la seguridad de los pacientes o la medicina personalizada. A fin de explotar plenamente los beneficios del uso secundario, todos los tenedores de datos de salud deben contribuir en este esfuerzo de poner a disposición para uso secundario las diferentes categorías de datos de salud electrónicos que tengan en su poder, siempre que dicho esfuerzo se realice mediante procesos eficaces y seguros, con el debido respeto de las obligaciones profesionales, incluidas, entre otras, las obligaciones de confidencialidad.

(56) Las categorías de datos de salud electrónicos que pueden tratarse para uso secundario deben ser lo suficientemente amplias y flexibles para responder a la evolución de las necesidades de los usuarios de datos de salud, al mismo tiempo que deben limitarse a los datos relacionados con la salud o cuya influencia en la salud sea conocida. También pueden incluir datos pertinentes del sistema sanitario, por ejemplo, historias clínicas electrónicas, datos de reclamaciones, datos de dispensaciones, datos de los registros de enfermedades o datos genómicos, así como datos con efectos sobre la salud, por ejemplo consumo de diferentes sustancias, situación socioeconómica o comportamiento, y datos sobre factores medioambientales tales como la contaminación, la radiación o el uso de determinadas sustancias químicas. Las categorías de datos de salud electrónicos para uso secundario incluyen

algunas categorías de datos que se recogieron principalmente para otros fines como la investigación, la elaboración de estadísticas, la seguridad de los pacientes, las actividades de regulación o formulación de políticas, por ejemplo, los registros de formulación de políticas o los registros relativos a los efectos secundarios de los medicamentos o los productos sanitarios. Existen bases de datos europeas que facilitan la utilización y reutilización de los datos en algunos ámbitos, como el cáncer (el Sistema Europeo de Información del Cáncer) o las enfermedades raras [por ejemplo, la Plataforma Europea para el Registro de Enfermedades Raras y los registros de las redes europeas de referencia (RER)]. Las categorías de datos de salud electrónicos que pueden ser tratadas para uso secundario deben incluir también datos generados automáticamente por productos sanitarios y por las personas, tales como los datos procedentes de aplicaciones de bienestar. Los datos sobre ensayos clínicos e investigaciones clínicas también deben incluirse en las categorías de datos de salud electrónicos para uso secundario cuando haya finalizado el ensayo clínico o la investigación clínica, sin que ello afecte a ningún intercambio voluntario de datos por parte de los promotores de ensayos e investigaciones en curso. Los datos de salud electrónicos para uso secundario deben ponerse a disposición preferentemente en un formato electrónico estructurado que facilite su tratamiento mediante sistemas informáticos. Como ejemplos de formatos electrónicos estructurados cabe citar los registros en una base de datos relacional, los documentos XML o los ficheros CSV y el texto libre, los audios, los vídeos y las imágenes proporcionados como archivos legibles por ordenador.

(57) Los usuarios de datos de salud que se beneficien del acceso a los conjuntos de datos proporcionados en virtud del presente Reglamento podrían enriquecer los datos de esos conjuntos de datos con diversas correcciones, anotaciones y otras mejoras, por ejemplo complementando los datos ausentes o incompletos, mejorando así la exactitud, exhaustividad o calidad de los datos de los conjuntos de datos. Se debe animar a los usuarios de datos de salud a que notifiquen a los organismos de acceso a datos de salud los errores críticos en los conjuntos de datos. Para contribuir a la mejora de la base de datos inicial y el uso ulterior del conjunto de datos enriquecido, los Estados miembros deben poder regular el tratamiento y uso de datos de salud electrónicos con disposiciones que contengan mejoras en relación con el tratamiento de esos datos. El conjunto de datos mejorado debe ponerse a disposición del tenedor de datos de salud original de forma gratuita junto con una descripción de las mejoras. El tenedor de datos de salud debe poner a disposición el nuevo conjunto de datos, a menos que notifique al organismo de acceso a datos de salud una justificación para no hacerlo, por ejemplo, cuando el enriquecimiento por parte del usuario de datos de salud es de baja calidad. También debe garantizarse la disponibilidad de datos de salud electrónicos no personales para uso secundario. En particular, los datos genómicos de patógenos tienen un valor significativo para la salud humana, como se ha puesto de relieve en la pandemia de COVID-19, durante la cual el acceso oportuno a dichos datos y su intercambio demostraron ser esenciales para el rápido desarrollo de herramientas de detección, contramedidas médicas y respuestas a las amenazas para la salud pública. Los mayores beneficios de los esfuerzos en genómica patógena se van a lograr cuando los procesos de salud pública y de investigación compartan conjuntos de datos y colaboren para informarse y mejorar mutuamente.

(58) Con el fin de aumentar la eficacia del uso secundario de los datos de salud electrónicos personales y de aprovechar plenamente las posibilidades que ofrece el presente Reglamento, la disponibilidad en el EEDS de los datos de salud electrónicos descritos en el capítulo IV debe ser tal que los datos sean tan accesibles, de elevada calidad, listos y adecuados para crear valor y calidad científicos, innovadores y sociales como sea posible. Los trabajos sobre la aplicación del EEDS y otras mejoras de los conjuntos de datos deben efectuarse de tal manera que se dé prioridad a los conjuntos de datos que sean los más adecuados para crear ese valor y calidad.

(59) Las entidades públicas o privadas reciben a menudo financiación pública, procedente de fondos nacionales o de la Unión, para recoger y tratar datos de salud electrónicos con fines de investigación, para estadísticas oficiales o no oficiales, o para otros fines similares, también en ámbitos en los que la recogida de tales datos está fragmentada o es difícil, tales como los relacionados con enfermedades raras o cáncer. Esos datos, que son recogidos y tratados por tenedores de datos de salud con apoyo de financiación pública de la Unión o nacional, deben ser puestos a disposición de los organismos de acceso a datos de salud, a fin de maximizar los efectos de la inversión pública y apoyar, en beneficio de la sociedad, la investigación, la innovación, la seguridad de los pacientes o la formulación de políticas. En algunos Estados miembros, las entidades privadas, incluidos los prestadores de asistencia sanitaria privados y las asociaciones profesionales, desempeñan un papel fundamental en el sector sanitario. Los datos de salud en poder de dichos prestadores también deben estar disponibles para uso secundario. Por tanto, los tenedores de datos de salud en el contexto del uso secundario deben ser entidades que sean prestadores de servicios sanitarios o asistenciales, que realicen investigaciones en relación con los sectores de la asistencia sanitaria o el asistencial, o desarrollen productos o servicios destinados a los sectores de la asistencia sanitaria o el asistencial. Esas entidades pueden ser públicas, sin ánimo de lucro o privadas. En consonancia con esa definición, las residencias de ancianos, los centros de día, las entidades que prestan servicios a personas con discapacidad, las entidades con actividades empresariales y tecnológicas relacionadas con la asistencia, como los ortopédicos y las empresas que prestan servicios asistenciales, deben considerarse tenedores de datos de salud. Las personas jurídicas que desarrollen aplicaciones de bienestar también deben ser consideradas tenedores de datos de salud. Las instituciones, órganos u organismos de la Unión que tratan dichas categorías de datos de salud y de datos de asistencia sanitaria, así como los registros de mortalidad, también deben considerarse tenedores de datos de salud. A fin de evitar una carga desproporcionada para las personas físicas y las microempresas, se les debe eximir, por regla general, de las

obligaciones que incumben a los tenedores de datos de salud. No obstante, los Estados miembros deben poder ampliar en su Derecho nacional las obligaciones de los tenedores de datos de salud a las personas físicas y a las microempresas. A fin de reducir la carga administrativa, y a la luz de los principios de eficacia y eficiencia, los Estados miembros deben poder exigir en su Derecho nacional que las entidades de intermediación de datos de salud desempeñen las funciones de determinadas categorías de tenedores de datos de salud. Dichas entidades de intermediación de datos de salud deben ser personas jurídicas capaces de tratar, poner a disposición, registrar, proporcionar, limitar el acceso e intercambiar datos de salud electrónicos para uso secundario proporcionados por los tenedores de datos. Esas entidades de intermediación de datos de salud realizan tareas diferentes a las de los servicios de intermediación de datos del Reglamento (UE) 2022/868.

(60) Los datos de salud electrónicos protegidos por derechos de propiedad intelectual e industrial o secretos comerciales, incluidos los datos sobre ensayos clínicos, investigaciones y estudios, pueden ser muy útiles para un uso secundario y pueden fomentar la innovación en la Unión en beneficio de los pacientes de la Unión. Con el fin de incentivar el liderazgo continuo de la Unión en este ámbito, es importante alentar el intercambio de datos sobre ensayos clínicos e investigaciones clínicas a través del EEDS para uso secundario. Los datos sobre ensayos clínicos e investigaciones clínicas deben estar disponibles en la medida de lo posible, al mismo tiempo que se adoptan todas las medidas necesarias para proteger los derechos de propiedad intelectual e industrial y los secretos comerciales. El presente Reglamento no debe utilizarse para reducir o eludir dicha protección y debe ser coherente con las disposiciones pertinentes en materia de transparencia establecidas en el Derecho de la Unión, incluidas las relativas a los datos de ensayos clínicos e investigaciones clínicas. Los organismos de acceso a datos de salud deben evaluar cómo preservar esa protección, permitiendo al mismo tiempo el acceso a dichos datos a los usuarios de datos de salud en la medida de lo posible. Si un organismo de acceso a datos de salud no puede proporcionar el acceso a dichos datos, debe informar al usuario de datos de salud y explicar por qué no es posible proporcionar dicho acceso. Las medidas legales, organizativas y técnicas para preservar los derechos de propiedad intelectual e industrial o los secretos comerciales podrían incluir acuerdos contractuales comunes de acceso a datos de salud electrónicos, obligaciones específicas en el permiso de datos en relación con dichos derechos, el tratamiento previo de los datos para generar datos derivados que protejan un secreto comercial, pero que sean útiles para el usuario de datos de salud o para la configuración del entorno de tratamiento seguro, de modo que el usuario de datos de salud no pueda acceder a dichos datos.

(61) El uso secundario de los datos de salud en el marco del EEDS debe permitir que las entidades públicas, privadas y sin ánimo de lucro, así como los investigadores individuales, tengan acceso a los datos de salud para la investigación, la innovación, la formulación de políticas, las actividades educativas, la seguridad de los pacientes, las actividades de regulación o la medicina personalizada, en consonancia con los fines establecidos en el presente Reglamento. El acceso a los datos para uso secundario debe contribuir al interés general de la sociedad. En particular, el uso secundario de los datos de salud con fines de investigación y desarrollo debe contribuir a beneficiar a la sociedad en forma de nuevos medicamentos, productos sanitarios y productos y servicios de asistencia sanitaria a precios asequibles y justos para los ciudadanos de la Unión, así como a mejorar el acceso a dichos productos y servicios y su disponibilidad en todos los Estados miembros. Las actividades para las que el acceso en el contexto del presente Reglamento es lícito pueden incluir el uso de datos de salud electrónicos para tareas realizadas por organismos del sector público, como el ejercicio de funciones públicas, incluida la vigilancia de la salud pública, las obligaciones de planificación y notificación, la formulación de políticas sanitarias, y la garantía de la seguridad de los pacientes, la calidad de la asistencia y la sostenibilidad de los sistemas sanitarios. Los organismos del sector público y las instituciones, órganos y organismos de la Unión pueden necesitar acceso periódico a los datos de salud electrónicos durante un período de tiempo prolongado, también para cumplir su mandato, tal como dispone el presente Reglamento. Los organismos del sector público pueden realizar esas actividades de investigación recurriendo a terceros, incluidos los subcontratistas, siempre que esos organismos sigan siendo en todo momento los supervisores de dichas actividades. El suministro de datos también debe apoyar actividades relacionadas con la investigación científica. El concepto de fines de investigación científica debe interpretarse de manera amplia, incluyendo el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada con fondos privados.Las actividades relacionadas con la investigación científica incluyen actividades de innovación tales como la formación de algoritmos de IA que podrían utilizarse en la asistencia sanitaria o la asistencia de personas físicas, así como la evaluación y el desarrollo ulterior de algoritmos y productos existentes para tales fines. Es necesario que el EEDS contribuya a la investigación fundamental y, aunque sus beneficios para los usuarios finales y los pacientes puedan ser menos directos, dicha investigación fundamental es crucial para los beneficios sociales a largo plazo. En algunos casos, la información de algunas personas físicas, como la información genómica de personas físicas con una enfermedad determinada, podría contribuir al diagnóstico o al tratamiento de otras. Es necesario que los organismos del sector público vayan más allá del ámbito de las «necesidades excepcionales» del capítulo V del Reglamento (UE) 2023/2854. No obstante, debe permitirse a los organismos de acceso a datos de salud prestar apoyo a organismos del sector público a la hora de tratar o vincular datos. El presente Reglamento proporciona un canal para que los organismos del sector público obtengan acceso a la información que necesitan para cumplir las misiones que les asigna la ley, pero no amplía el mandato de dichos organismos del sector público.

(62) Debe prohibirse cualquier intento de utilizar los datos de salud electrónicos para medidas perjudiciales para las personas físicas, tales como aumentar las primas de seguro, desarrollar actividades perjudiciales para las personas físicas relacionadas con el empleo, las pensiones o el sector bancario, incluidas las hipotecas sobre bienes inmuebles, anunciar productos o tratamientos, automatizar la toma de decisiones individuales, reidentificar a personas físicas o desarrollar productos nocivos. Esa prohibición debe aplicarse a las actividades contrarias a las disposiciones éticas del Derecho nacional, con excepción de las disposiciones éticas relativas al consentimiento del interesado al tratamiento de datos personales y las disposiciones éticas relativas al derecho de autoexclusión, ya que el presente Reglamento prevalece sobre el Derecho nacional de conformidad con el principio general de primacía del Derecho de la Unión. Debe prohibirse también proporcionar acceso a los datos de salud electrónicos a terceros no mencionados en el permiso de datos, o ponerlos a su disposición de algún otro modo. Debe indicarse en el permiso de datos la identidad de las personas autorizadas, en particular la identidad del investigador principal, que tendrán derecho a acceder a los datos de salud electrónicos en el entorno de tratamiento seguro en virtud del presente Reglamento. Los investigadores principales son las principales personas responsables de solicitar el acceso a los datos de salud electrónicos y de tratar los datos solicitados en el entorno de tratamiento seguro en nombre del usuario de datos de salud.

(63) El presente Reglamento no crea unas facultades de uso secundario de datos de salud con fines policiales. La prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales por parte de las autoridades competentes no deben figurar dentro de los fines de uso secundario con arreglo al presente Reglamento. Por consiguiente, los órganos jurisdiccionales y otras entidades del sistema judicial no deben considerarse usuarios de datos de salud en el uso secundario de los datos de salud en virtud del presente Reglamento. Además, los órganos jurisdiccionales y otras entidades del sistema judicial no deben estar cubiertos por la definición de tenedores de datos de salud y, por tanto, no deben ser destinatarios de las obligaciones que incumben a los tenedores de datos de salud en virtud del presente Reglamento. Además, las facultades de las autoridades competentes en materia de prevención, investigación, detección y enjuiciamiento de infracciones penales establecidas por ley para obtener datos de salud electrónicos no se ven afectadas por el presente Reglamento. Del mismo modo, los datos de salud electrónicos en poder de los órganos jurisdiccionales a efectos de procedimientos judiciales quedan fuera del ámbito de aplicación del presente Reglamento.

(64) La creación de uno o varios organismos de acceso a datos de salud, que faciliten el acceso a los datos de salud electrónicos en los Estados miembros, es esencial para promover el uso secundario de los datos relacionados con la salud. Por consiguiente, los Estados miembros deben crear uno o varios organismos de acceso a datos de salud para reflejar, entre otras cosas, su estructura constitucional, organizativa y administrativa. Sin embargo, uno de esos organismos de acceso a datos de salud debe ser designado coordinador en caso de que haya más de un organismo de acceso a datos de salud. Cuando un Estado miembro establezca varios organismos de acceso a datos de salud, debe establecer reglas a nivel nacional para garantizar la participación coordinada de dichos organismos en el Consejo del Espacio Europeo de Datos de Salud (en lo sucesivo, «Consejo del EEDS»). Tal Estado miembro debe, en particular, designar un organismo de acceso a datos de salud que funcione como punto de contacto único de cara a la participación efectiva de tales organismos, y garantizar una cooperación rápida y fluida con otros organismos de acceso a datos de salud, el Consejo del EEDS y la Comisión. Los organismos de acceso a datos de salud pueden variar en términos de organización y tamaño, desde una organización de pleno derecho a una unidad o departamento de una organización existente. Los organismos de acceso a datos de salud no deben verse influidos en sus decisiones sobre el acceso a datos electrónicos para uso secundario y deben evitar cualquier conflicto de intereses. Por tanto, los miembros de los órganos decisorios y de gobierno de cada organismo de acceso a datos de salud y su personal deben abstenerse de cualquier acción que sea incompatible con sus funciones y no deben participar en ninguna actividad que sea incompatible.Sin embargo, la independencia de los organismos de acceso a datos de salud no debe significar que no puedan estar sometidos a mecanismos de control o seguimiento de su gasto financiero o a control jurisdiccional. Cada organismo de acceso a datos de salud debe estar dotado de los recursos financieros, técnicos y humanos, los locales y la infraestructura que sean necesarios para la realización eficaz de sus funciones, incluidas las relacionadas con la cooperación con otros organismos de acceso a datos de salud de toda la Unión. Los miembros de los órganos decisorios y de gobierno de los organismos de acceso a datos de salud y su personal deben tener las cualificaciones, experiencia y capacidades necesarias. Cada organismo de acceso a datos de salud debe disponer de un presupuesto anual público propio, que puede formar parte del presupuesto general del Estado o de otro ámbito nacional. A fin de permitir un mejor acceso a los datos de salud y complementar el artículo 7, apartado 2, del Reglamento (UE) 2022/868, los Estados miembros deben confiar a los organismos de acceso a datos de salud competencias para tomar decisiones sobre el acceso a datos de salud y sobre su uso secundario. Esto podría consistir en asignar nuevas funciones a los organismos competentes designados por los Estados miembros con arreglo al artículo 7, apartado 1, del Reglamento (UE) 2022/868 o en designar a organismos sectoriales existentes o nuevos como responsables de dichas funciones en relación con el acceso a datos de salud.

(65) Los organismos de acceso a datos de salud deben supervisar la aplicación del capítulo IV del presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, los organismos de acceso a datos de salud deben cooperar entre ellos y con la Comisión. Los organismos de acceso a datos de salud también deben cooperar con las partes interesadas, incluidas las organizaciones de pacientes. Los organismos de acceso a datos de salud deben apoyar

a los tenedores de datos de salud que sean pequeñas empresas de conformidad con la Recomendación 2003/361/CE de la Comisión ([18]), en particular a los médicos y las farmacias. Dado que el uso secundario de los datos de salud implica el tratamiento de datos personales relativos a la salud, son de aplicación las disposiciones pertinentes de los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y las autoridades de control en virtud de dichos Reglamentos deben seguir siendo las únicas autoridades competentes para hacer cumplir esas disposiciones. Los organismos de acceso a datos de salud deben informar a las autoridades de protección de datos de cualquier sanción impuesta y de cualquier posible cuestión relacionada con el tratamiento de datos para uso secundario e intercambiar toda la información pertinente de que dispongan para garantizar el cumplimiento de las normas pertinentes. Además de las funciones necesarias para garantizar un uso secundario eficaz de los datos de salud, los organismos de acceso a datos de salud deben esforzarse por ampliar la disponibilidad de conjuntos de datos de salud adicionales y promover el desarrollo de normas comunes. Deben aplicar técnicas probadas de última generación que aseguren que los datos de salud electrónicos para los que se permite un uso secundario se traten de forma que se preserve la privacidad de la información que contienen, como son las técnicas de seudonimización, anonimización, generalización, supresión y aleatorización de datos personales. Los organismos de acceso a datos de salud pueden elaborar conjuntos de datos vinculados para los usuarios de datos de salud tal como se exija en el marco del permiso de datos expedido. A este respecto, los organismos de acceso a datos de salud deben cooperar de forma transfronteriza e intercambiar las mejores prácticas y técnicas. Esto incluye reglas para la seudonimización y la anonimización de conjuntos de microdatos. Cuando sea necesario, la Comisión debe establecer los procedimientos y requisitos, y proporcionar las herramientas técnicas para un procedimiento unificado de seudonimización y anonimización de los datos de salud electrónicos.

(66) Los organismos de acceso a datos de salud deben garantizar que el uso secundario sea transparente, para lo cual deben proporcionar información pública sobre los permisos de datos concedidos y sus justificaciones, las medidas adoptadas para proteger los derechos de las personas físicas, el modo en que las personas físicas pueden ejercer sus derechos en relación con el uso secundario, y los resultados del uso secundario, también mediante enlaces a publicaciones científicas. Cuando proceda, esa información sobre los resultados del uso secundario también debe incluir un resumen de la situación que debe aportar el usuario de datos de salud. Esas obligaciones de transparencia complementan las obligaciones previstas en el artículo 14 del Reglamento (UE) 2016/679. Pueden aplicarse las excepciones previstas en el artículo 14, apartado 5, de dicho Reglamento. Cuando tales excepciones sean aplicables, las obligaciones de transparencia establecidas en el presente Reglamento deben contribuir a garantizar un tratamiento leal y transparente, tal como se contempla en el artículo 14, apartado 2, del Reglamento (UE) 2016/679, por ejemplo, mediante el suministro de información sobre los fines del tratamiento y las categorías de datos tratados, lo que permite a las personas físicas comprender si sus datos se ponen a disposición para un uso secundario con arreglo a los permisos de datos.

(67) Las personas físicas deben ser informadas por los tenedores de datos de salud de los hallazgos significativos relacionadas con su salud que hayan sido realizadas por los usuarios de datos de salud. Las personas físicas deben tener derecho a solicitar que no se las informe de tales constataciones. Los Estados miembros podrían establecer condiciones en cuanto a las modalidades por las que los tenedores de datos de salud proporcionen tal información a las personas físicas de que se trate y en cuanto al ejercicio del derecho a no ser informado. De conformidad con el artículo 23, apartado 1, letra i), del Reglamento (UE) 2016/679, los Estados miembros deben poder limitar el alcance de la obligación de informar a las personas físicas siempre que sea necesario para su protección, en consideración de la seguridad de los pacientes y la ética, retrasando la comunicación de su información hasta que un profesional sanitario pueda comunicar y explicar a las personas físicas de que se trate la información que pueda tener consecuencias para su salud.

(68) A fin de promover la transparencia, los organismos de acceso a datos de salud deben publicar un informe bienal de actividad que ofrezca una síntesis de sus actividades. Cuando un Estado miembro haya designado más de un organismo de acceso a datos de salud, el organismo coordinador debe elaborar y publicar un informe común bienal. Los informes de actividades deben seguir una estructura acordada por el Consejo del EEDS y ofrecer una síntesis de las actividades, que incluya información sobre las decisiones sobre solicitudes, auditorías y el compromiso con las partes interesadas pertinentes. Entre estas partes interesadas pueden figurar representantes de personas físicas, organizaciones de pacientes, profesionales sanitarios, investigadores y comités éticos.

(69) A fin de apoyar el uso secundario, los tenedores de datos de salud deben abstenerse de retener los datos, de solicitar tasas injustificadas que no sean transparentes ni proporcionadas a los costes de puesta a disposición de los datos, o, cuando proceda, a los costes marginales de la recogida de datos, y de solicitar a los usuarios de datos de salud que copubliquen las investigaciones u otras prácticas que puedan disuadirlos de pedir los datos. Cuando un tenedor de datos de salud sea un organismo del sector público, la parte de las tasas vinculada a sus costes no debe cubrir los

([18]) Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

costes de la recogida inicial de los datos. Cuando sea necesaria una aprobación ética para proporcionar un permiso de datos, la evaluación relativa a la aprobación ética debe basarse en sus propios méritos.

(70) Debe permitirse que los organismos de acceso a datos de salud cobren tasas por las funciones que realizan, teniendo en cuenta las disposiciones horizontales previstas por el Reglamento (UE) 2022/868. Estas tasas pueden tener en cuenta la situación y los intereses de las pequeñas y medianas empresas (pymes), los investigadores individuales o los organismos del sector público. En particular, los Estados miembros deben poder establecer medidas para los organismos de acceso a datos de salud bajo su jurisdicción que hagan posible el cobro de tasas reducidas a determinadas categorías de usuarios de datos de salud. Los organismos de acceso a datos de salud deben poder cubrir los costes de sus actividades con tasas establecidas de manera proporcionada, justificada y transparente. Esto puede dar lugar a tasas más elevadas para algunos usuarios de datos de salud, si la tramitación de sus solicitudes de acceso a datos de salud y peticiones de datos de salud requiere más trabajo. También debe permitirse que los tenedores de datos de salud requieran tasas que reflejen los costes por la puesta a disposición de los datos. Los organismos de acceso a datos de salud deben decidir el importe de esas tasas, que también podrían incluir las tasas solicitadas por el tenedor de datos de salud. Esas tasas deberían ser cobradas por el organismo de acceso a datos de salud al usuario de datos de salud en una única factura. A continuación, el organismo de acceso a datos de salud debe transferir la parte pertinente de las tasas pagadas al tenedor de datos de salud. A fin de garantizar un enfoque armonizado en relación con las políticas y la estructura de las tasas, deben conferirse a la Comisión competencias de ejecución. El artículo 10 del Reglamento (UE) 2023/2854 debe aplicarse a las tasas cobradas en virtud del presente Reglamento.

(71) Con el fin de reforzar el cumplimiento de las disposiciones sobre el uso secundario, deben preverse medidas adecuadas que puedan dar lugar a multas administrativas o medidas de garantía del cumplimiento impuestas por los organismos de acceso a datos de salud o exclusiones temporales o definitivas del marco del EEDS de los usuarios de datos de salud o de los tenedores de datos de salud que no cumplan sus obligaciones. Los organismos de acceso a datos de salud deben estar facultados para verificar el cumplimiento por parte de los usuarios de datos de salud y de los tenedores de datos de salud, y darles la oportunidad de responder a cualquier constatación y de subsanar cualquier infracción. A la hora de decidir la cuantía de la multa administrativa o medida de garantía del cumplimiento para cada caso concreto, los organismos de acceso a datos de salud deben tener en cuenta los márgenes de costes y los criterios establecidos en el presente Reglamento, garantizando así que dichas multas o medidas son proporcionadas.

(72) Dada la sensibilidad de los datos de salud electrónicos, es necesario reducir los riesgos para la privacidad de las personas físicas aplicando el principio de minimización de datos. Por lo tanto, deben estar disponibles datos de salud electrónicos no personales siempre que su suministro resulte suficiente. Si el usuario de datos de salud necesita utilizar datos de salud electrónicos personales, debe indicar claramente en su petición la justificación del uso de ese tipo de datos y el organismo de acceso a datos de salud debe evaluar si dicha justificación es válida. Los datos de salud electrónicos personales solo deben estar disponibles en formato seudonimizado. Teniendo en cuenta los fines específicos del tratamiento, los datos electrónicos personales deben seudonimizarse o anonimizarse lo antes posible en el proceso de puesta a disposición de datos para uso secundario. La seudonimización y la anonimización deben poder realizarlas los organismos de acceso a datos de salud o los tenedores de datos de salud. Como responsables del tratamiento, los organismos de acceso a datos de salud y los tenedores de datos de salud deber poder delegar esas funciones en los encargados del tratamiento. Al proporcionar acceso a un conjunto de datos seudonimizado o anonimizado, un organismo de acceso a datos de salud debe utilizar las normas o las tecnologías de anonimización o seudonimización de última generación, que garanticen en la mayor medida posible que los usuarios de datos de salud no puedan reidentificar a las personas físicas. Esas tecnologías y normas para la anonimización de datos deben seguir desarrollándose. Los usuarios de datos de salud no deben intentar reidentificar a las personas físicas del conjunto de datos proporcionado en virtud del presente Reglamento, y, en caso de hacerlo, deber ser objeto de multas administrativas y las medidas de garantía del cumplimiento establecidas en el presente Reglamento o a posibles sanciones penales, cuando el Derecho nacional así lo prevea. Además, el solicitante de datos de salud debe poder solicitar una respuesta a una petición de datos de salud en formato estadístico anonimizado. En tales casos, el usuario de datos de salud solo trata datos no personales y el organismo de acceso a datos de salud sigue siendo el único responsable del tratamiento de todos los datos personales necesarios para responder a la petición de datos de salud.

(73) Con el fin de garantizar que todos los organismos de acceso a datos de salud expidan permisos de datos de manera similar, es necesario establecer un proceso común normalizado para la expedición de permisos de datos, con peticiones similares en diferentes Estados miembros. El solicitante de datos de salud debe proporcionar a los organismos de acceso a datos de salud varios elementos de información que los ayuden a evaluar la solicitud de acceso a datos de salud y decidir si el solicitante de datos de salud puede recibir un permiso de datos, y debe garantizarse la coherencia entre los distintos organismos de acceso a datos de salud. La información proporcionada

como parte de la solicitud de acceso a datos de salud debe cumplir los requisitos establecidos en el presente Reglamento para posibilitar que sea evaluada de forma exhaustiva, ya que solo debe expedirse un permiso de datos si se cumplen todas las condiciones necesarias establecidas en el presente Reglamento. Además, cuando proceda, dicha información debe incluir una declaración del solicitante de datos de salud en la que se disponga que el uso previsto de los datos solicitados no entraña un riesgo de estigmatización o un perjuicio para la dignidad de las personas físicas ni para los grupos relacionados con el conjunto de datos solicitado. Podrá solicitarse una evaluación ética con arreglo al Derecho nacional. En tal caso, los organismos de ética existentes deben poder efectuar estas evaluaciones para el organismo de acceso a datos de salud. Los organismos de ética existentes de los Estados miembros deben poner sus conocimientos especializados a disposición del organismo de acceso a datos de salud para ese fin. Alternativamente, los Estados miembros deben poder disponer que los organismos de ética sean parte del organismo de acceso a datos de salud. El organismo de acceso a datos de salud y, en su caso, los tenedores de datos de salud deben ayudar a los usuarios de datos de salud en la selección de los conjuntos de datos o fuentes de datos adecuados para la finalidad prevista de uso secundario. Cuando el solicitante de datos de salud necesite datos en un formato estadístico anonimizado, debe presentar una petición datos de salud, en la que se pida al organismo de acceso a datos de salud que proporcione directamente el resultado. La denegación de un permiso de datos por parte del organismo de acceso a datos de salud no debe impedir que el solicitante de datos de salud presente una nueva solicitud de acceso a datos de salud. A fin de garantizar un enfoque armonizado entre los organismos de acceso a datos de salud y limitar la carga administrativa para los solicitantes de datos de salud, la Comisión debe apoyar la armonización de las solicitudes de acceso a datos de salud, así como de las peticiones de datos de salud, también mediante el establecimiento de los modelos pertinentes. En casos justificados, como el de una petición compleja y gravosa, se debe permitir al organismo de acceso a datos de salud ampliar el plazo para que los tenedores de datos de salud pongan los datos de salud electrónicos que se han pedido a disposición de dicho organismo.

(74) Dado que los recursos de los organismos de acceso a los datos de salud son limitados, dichos organismos deben poder aplicar reglas de prioridad, por ejemplo dando prioridad a las instituciones públicas ante las entidades privadas, pero no deben discriminar entre organizaciones nacionales y de otros Estados miembros dentro de la misma categoría de prioridades. El usuario de datos de salud debe poder prorrogar la duración del permiso de datos para, por ejemplo, permitir el acceso a conjuntos de datos a los revisores de publicaciones científicas o permitir un análisis adicional del conjunto de datos sobre la base de los resultados iniciales. Para ello se debe exigir una modificación del permiso de datos y puede ser objeto de una tasa adicional. Sin embargo, en todos los casos, el permiso de datos debe reflejar esos usos adicionales del conjunto de datos. Preferiblemente, el usuario de datos de salud debe mencionarlos en su solicitud inicial de acceso a datos de salud. A fin de garantizar un enfoque armonizado entre los organismos de acceso a datos de salud, la Comisión debe apoyar la armonización de los permisos de datos.

(75) Como ha puesto de manifiesto la crisis de la COVID-19, las instituciones, órganos y organismos de la Unión con un mandato legal en el ámbito de la salud pública, especialmente la Comisión, necesitan acceder a los datos de salud durante un período más largo y de forma recurrente. Este puede ser el caso no solo en circunstancias específicas establecidas en el Derecho de la Unión o nacional en tiempos de crisis, sino también para proporcionar periódicamente pruebas científicas y apoyo técnico a las políticas de la Unión. Puede exigirse el acceso a dichos datos en determinados Estados miembros o en todo el territorio de la Unión. Tales instituciones, órganos y organismos de la Unión deben poder beneficiarse de un procedimiento acelerado de modo que los datos estén disponibles habitualmente en menos de dos meses, con la posibilidad de que el plazo se prolongue un mes más en los casos más complejos.

(76) Los Estados miembros deben poder designar tenedores fiables de datos de salud para los que el procedimiento de expedición de permiso de datos pueda realizarse de manera simplificada, a fin de aligerar la carga administrativa que supone para los organismos de acceso a datos de salud la gestión de las peticiones de datos que tratan. Los tenedores fiables de datos de salud deben poder evaluar las solicitudes de acceso a datos de salud presentadas con arreglo a este procedimiento simplificado, sobre la base de su experiencia en la gestión del tipo de datos de salud que están tratando, y emitir una recomendación relativa a un permiso de datos. El organismo de acceso a datos de salud debe seguir siendo responsable de la expedición del permiso de datos final y no debe estar vinculado por la recomendación formulada por el tenedor fiable de datos de salud. Las entidades de intermediación de datos de salud no deben ser designadas tenedores fiables de datos de salud.

(77) Dada la sensibilidad de los datos de salud electrónicos, los usuarios de datos de salud no deben tener acceso ilimitado a dichos datos. Todo acceso de uso secundario a los datos de salud electrónicos en respuesta a una petición debe hacerse a través de un entorno de tratamiento seguro. A fin de garantizar que existen garantías técnicas y de seguridad sólidas para los datos de salud electrónicos, el organismo de acceso a datos de salud o, en su caso, el tenedor fiable de datos de salud debe proporcionar acceso a dichos datos en un entorno de tratamiento seguro, cumpliendo las estrictas normas técnicas y de seguridad establecidas en virtud del presente Reglamento. El tratamiento de datos personales en dicho entorno de tratamiento seguro debe cumplir lo dispuesto en el Reglamento (UE) 2016/679, incluidos, cuando el entorno de tratamiento seguro sea gestionado por un tercero, los requisitos del

artículo 28 y, en su caso, del capítulo V de dicho Reglamento. Ese entorno de tratamiento seguro debe reducir los riesgos para la privacidad relacionados con dichas actividades de tratamiento e impedir que los datos de salud electrónicos se transmitan directamente a los usuarios de datos de salud. El organismo de acceso a datos de salud o el tenedor de datos de salud que preste ese servicio debe seguir controlando en todo momento el acceso a datos de salud electrónicos y el acceso concedido a los usuarios de datos de salud deber determinarse en función de las condiciones del permiso de datos expedido. Solo los datos de salud electrónicos no personales que no contengan datos de salud electrónicos personales deben ser descargados por los usuarios de datos de salud de dicho entorno de tratamiento seguro. Por lo tanto, dicho entorno de tratamiento seguro es una garantía esencial para proteger los derechos y las libertades de las personas físicas en relación con el tratamiento de sus datos de salud electrónicos para uso secundario. La Comisión debe ayudar a los Estados miembros a elaborar normas comunes de seguridad con el fin de promover la seguridad y la interoperabilidad de los distintos entornos de tratamiento seguros.

(78) El Reglamento (UE) 2022/868 establece la normativa general para la gestión de la cesión altruista de datos. Dado que el sector sanitario gestiona datos sensibles, deben establecerse criterios adicionales a través del código normativo a que se refiere dicho Reglamento. Cuando dicha normativa disponga el uso de un entorno de tratamiento seguro para ese sector, dicho entorno de tratamiento seguro debe cumplir los criterios establecidos en el presente Reglamento. Los organismos de acceso a datos de salud deben cooperar con las autoridades competentes designadas en virtud del Reglamento (UE) 2022/868 para supervisar la actividad de las organizaciones de cesión altruista de datos en el sector sanitario o asistencial.

(79) Para el tratamiento de datos de salud electrónicos en el ámbito de un permiso de datos o una petición de datos de salud, los tenedores de datos de salud, incluidos los tenedores fiables de datos de salud, los organismos de acceso a datos de salud y los usuarios de datos de salud deben ser considerados, a su vez, responsables del tratamiento de una parte específica del tratamiento y de conformidad con sus respectivas funciones en él. Los tenedores de datos de salud deben ser considerados responsables del tratamiento para la divulgación de los datos de salud electrónicos personales solicitados al organismo de acceso a datos de salud, mientras que los organismos de acceso a datos de salud deben, a su vez, ser considerados responsables del tratamiento de los datos de salud electrónicos personales cuando preparen los datos y los pongan a disposición de los usuarios de datos de salud. Los usuarios de datos de salud deben ser considerados responsables del tratamiento de los datos de salud electrónicos personales en forma seudonimizada en el entorno de tratamiento seguro en virtud de sus permisos de datos. Los organismos de acceso a datos de salud deben ser considerados encargados del tratamiento, en nombre del usuario de datos de salud, para el tratamiento realizado por el usuario de datos de salud en virtud de un permiso de datos en el entorno de tratamiento seguro, así como para el tratamiento para generar una respuesta a una petición de datos de salud. Del mismo modo, los tenedores fiables de datos de salud deben ser considerados responsables del tratamiento de datos de salud electrónicos personales en relación con el suministro de datos de salud electrónicos al usuario de datos de salud con arreglo a un permiso de datos o a una petición de datos de salud. Debe considerarse que los tenedores fiables de datos de salud actúan como encargados del tratamiento por parte del usuario de datos de salud cuando proporcionen datos a través de un entorno de tratamiento seguro.

(80) Con el fin de lograr un marco integrador y sostenible para el uso secundario plurinacional, debe crearse una infraestructura transfronteriza [«DatosSalud@UE» (*HealthData@EU*)]. DatosSalud@UE debe acelerar el uso secundario, aumentando al mismo tiempo la seguridad jurídica, respetando la privacidad de las personas físicas y siendo interoperable. Debido a la sensibilidad de los datos de salud, deben respetarse, siempre que sea posible, principios como el de «protección de la privacidad desde el diseño» y el de «protección de la privacidad por defecto», así como el concepto de «interrogar datos en lugar de trasladar datos». Los Estados miembros deben designar puntos de contacto nacionales para el uso secundario, como pasarelas tanto organizativas como técnicas para los organismos de acceso a datos de salud, y conectar esos puntos de contacto a DatosSalud@UE. El servicio de acceso a datos de salud de la Unión también debe estar conectado a DatosSalud@UE. Además, los participantes autorizados en DatosSalud@UE pueden ser infraestructuras de investigación establecidas como un Consorcio de Infraestructuras de Investigación Europeas (ERIC, por sus siglas en inglés) en virtud del Reglamento (CE) n.º 723/2009 del Consejo ([19]), como un Consorcio de Infraestructuras Digitales Europeas (EDIC, por sus siglas en inglés) en virtud de la Decisión (UE) 2022/2481 o infraestructuras similares establecidas en virtud de otros actos jurídicos de la Unión, así como otros tipos de entidades, incluidas las infraestructuras del Foro Estratégico Europeo sobre Infraestructuras de Investigación (ESFRI, por sus siglas en inglés), o las infraestructuras federadas en el marco de la Nube Europea de la Ciencia Abierta (EOSC, por sus siglas en inglés). Los terceros países y las organizaciones internacionales también podrían convertirse en participantes autorizados en DatosSalud@UE, siempre que cumplan los requisitos del presente Reglamento. La Comunicación de la Comisión, de 19 de febrero de 2020, titulada «Una Estrategia Europea de Datos» fomentaba la conexión de los distintos espacios comunes europeos de datos. Por lo tanto, DatosSalud@UE debe permitir el uso secundario de diferentes categorías de datos de salud electrónicos, incluida la vinculación de los datos de salud con los de otros espacios de datos, como los relaciones con el medio ambiente, la agricultura y el sector social. Esa interoperabilidad entre el sector sanitario y otros sectores como el medioambiental, el agrícola o el social podría ser pertinente para obtener información adicional sobre los factores determinantes de la salud. La

([19]) Reglamento (CE) n.º 723/2009 del Consejo, de 25 de junio de 2009, relativo al marco jurídico comunitario aplicable a los Consorcios de Infraestructuras de Investigación Europeas (ERIC) (DO L 206 de 8.8.2009, p. 1).

Comisión podría ofrecer una serie de servicios dentro de DatosSalud@UE, incluido el apoyo para el intercambio de información entre los organismos de acceso a datos de salud y los participantes autorizados en DatosSalud@UE para la tramitación de las solicitudes de acceso transfronterizo, el mantenimiento de los catálogos de datos de salud electrónicos disponibles a través de la infraestructura, la posibilidad de descubrir redes y las consultas de metadatos, y los servicios de conectividad y cumplimiento. La Comisión también podría crear un entorno de tratamiento seguro que permita transmitir y analizar datos procedentes de diferentes infraestructuras nacionales, a petición de los responsables del tratamiento. En aras de la eficiencia informática, la racionalización y la interoperabilidad de los intercambios de datos, los sistemas existentes de intercambio de datos deben reutilizarse todo lo que sea posible, como los que se están construyendo para el intercambio de pruebas en el marco del «sistema técnico basado en el principio de "solo una vez"» del Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo ([20]).

(81) Además, dado que la conexión a DatosSalud@UE podría implicar transferencias a terceros países de datos personales relacionados con el solicitante o usuario de datos de salud, es necesario disponer de instrumentos de transferencia pertinentes de conformidad con el capítulo V del Reglamento (UE) 2016/679 para dichas transferencias.

(82) En el caso de registros o bases de datos transfronterizos, como los registros de las redes europeas de referencia para enfermedades raras, que reciben datos de diferentes prestadores de asistencia sanitaria en varios Estados miembros, el organismo de acceso a datos de salud del Estado miembro en el que esté situado el coordinador del registro debe ser el responsable de proporcionar el acceso a los datos.

(83) El proceso de autorización para acceder a datos de salud electrónicos personales en diferentes Estados miembros puede ser repetitivo y engorroso para los usuarios de datos de salud. Siempre que sea posible, deben establecerse sinergias para reducir la carga y las barreras para los usuarios de datos de salud. Una manera de lograr dicho objetivo es sumarse al principio de «solicitud única», según el cual, con una solicitud, el usuario de datos de salud puede obtener la autorización de múltiples organismos de acceso a datos de salud de diferentes Estados miembros o participantes autorizados en DatosSalud@UE.

(84) Los organismos de acceso a datos de salud deben proporcionar información sobre los conjuntos de datos disponibles y sus características, de modo que los usuarios de datos de salud puedan informarse de los hechos elementales sobre el conjunto de datos y evaluar la posible pertinencia de los hechos para esos usuarios. Por este motivo, cada conjunto de datos debe incluir, como mínimo, información sobre la fuente y la naturaleza de los datos así como las condiciones para su puesta a disposición. El tenedor de datos de salud debe comprobar, al menos una vez al año, que su descripción de los conjuntos de datos en el catálogo nacional de conjuntos de datos es exacta y está actualizada. Por consiguiente, debe establecerse un catálogo de conjuntos de datos de la UE para facilitar la posibilidad de descubrir los conjuntos de datos disponibles en el EEDS; ayudar a los tenedores de datos de salud a publicar sus conjuntos de datos; proporcionar a todas las partes interesadas, incluida la población general, teniendo también en cuenta las necesidades específicas de las personas con discapacidad, información sobre los conjuntos de datos introducidos en el EEDS (como etiquetas de calidad y utilidad, y fichas de información sobre los conjuntos de datos), y proporcionar a los usuarios de datos de salud información actualizada sobre la calidad de los datos y sobre la utilidad de los conjuntos de datos.

(85) La información sobre la calidad y la utilidad de los conjuntos de datos aumenta significativamente el valor de los resultados de la investigación y la innovación intensivas en datos, al mismo tiempo que promueve la toma de decisiones de regulación y formulación de políticas basándose en datos contrastados. Las mejoras en la calidad y la utilidad de los conjuntos de datos mediante una elección fundada del cliente y la armonización de los requisitos conexos a escala de la Unión, teniendo en cuenta las normas, directrices y recomendaciones de la Unión e internacionales existentes para la recogida y el intercambio de datos (por ejemplo, los principios FAIR) también benefician a los tenedores de datos de salud, los profesionales sanitarios, las personas físicas y la economía de la Unión en general. Una etiqueta de calidad y utilidad de los datos para los conjuntos de datos informaría a los usuarios de datos de salud sobre las características de un conjunto de datos en cuanto a calidad y utilidad y les permitiría elegir los conjuntos de datos que mejor se ajusten a sus necesidades. La etiqueta de calidad y utilidad de los datos no debe impedir que los conjuntos de datos estén disponibles a través del EEDS, sino proporcionar un mecanismo de transparencia entre los tenedores de datos de salud y los usuarios de datos de salud. Por ejemplo, un conjunto de datos que no cumpla ningún requisito de calidad y utilidad de los datos debe etiquetarse con la categoría que represente la calidad y la utilidad más pobres, pero debe seguir estando disponible. A la hora de desarrollar el marco de calidad y utilidad de los datos, deben tenerse en cuenta las expectativas generadas por los marcos creados con arreglo al artículo 10 del Reglamento (UE) 2024/1689 y la documentación técnica pertinente especificada en el anexo IV de dicho Reglamento. Los Estados miembros deben fomentar la concienciación sobre la etiqueta de calidad y utilidad de los datos a través de actividades de comunicación. La Comisión podría apoyar dichas actividades. Los usuarios podrían dar prioridad al uso de conjuntos de datos en función de su utilidad y calidad.

([20]) Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012 (DO L 295 de 21.11.2018, p. 1).

(86) El catálogo de conjuntos de datos de la UE debe reducir al mínimo la carga administrativa para los tenedores de datos de salud y otros usuarios de las bases de datos, también debe ser fácil de utilizar, accesible y eficiente en términos de costes, conectar los catálogos nacionales de conjuntos de datos y evitar el registro redundante de conjuntos de datos. Sin perjuicio de los requisitos establecidos en el Reglamento (UE) 2022/868, el catálogo de conjuntos de datos de la UE podría adaptarse a la iniciativa data.europa.eu. Debe garantizarse la interoperabilidad entre el catálogo de conjuntos de datos de la UE, los catálogos nacionales de conjuntos de datos y los catálogos de conjuntos de datos de las infraestructuras de investigación europeas y otras infraestructuras pertinentes de intercambio de datos.

(87) Existe actualmente una cooperación y trabajo entre diferentes organizaciones profesionales, la Comisión y otras instituciones para establecer campos de datos mínimos y otras características de los diferentes conjuntos de datos, por ejemplo, los registros. Ese trabajo está más avanzado en ámbitos como el cáncer, las enfermedades raras, las enfermedades cardiovasculares y metabólicas, la evaluación de los factores de riesgo y las estadísticas, y debe tenerse en cuenta a la hora de definir nuevas normas y modelos armonizados específicos para determinadas enfermedades para elementos de datos estructurados. Sin embargo, muchos conjuntos de datos no están armonizados, lo que plantea problemas de comparabilidad y dificulta la investigación transfronteriza. Por consiguiente, deben establecerse disposiciones más detalladas en actos de ejecución para garantizar la armonización de la codificación y el registro de datos de salud electrónicos a fin de permitir el suministro de tales datos para uso secundario de manera coherente. Esos conjuntos de datos pueden incluir datos de registros de enfermedades raras, bases de datos sobre medicamentos huérfanos, registros de cáncer y registros de enfermedades infecciosas de gran importancia. Los Estados miembros deben actuar para garantizar que los sistemas y servicios europeos de sanidad electrónica y las aplicaciones interoperables generen beneficios económicos y sociales sostenibles, con miras a alcanzar un alto grado de confianza y seguridad, mejorar la continuidad de la asistencia sanitaria y garantizar que el acceso a esta sea seguro y de calidad. Las infraestructuras de datos de salud y los registros existentes pueden proporcionar modelos que resulten útiles a la hora de determinar y aplicar normas sobre datos y la interoperabilidad, y deben utilizarse para permitir la continuidad y aprovechar los conocimientos especializados existentes.

(88) La Comisión debe apoyar a los Estados miembros en el desarrollo de las capacidades y la mejora de la eficacia en el ámbito de los sistemas sanitarios digitales para el uso primario y el uso secundario. Los Estados miembros deben recibir apoyo para reforzar su capacidad. Las actividades a escala de la Unión, como la evaluación comparativa y el intercambio de mejores prácticas, son medidas pertinentes a ese respecto. Esas actividades deben tener en cuenta las circunstancias específicas de las diferentes categorías de partes interesadas, como los representantes de la sociedad civil, los investigadores, las asociaciones médicas y las pymes.

(89) Mejorar la alfabetización sanitaria digital de las personas físicas y de los profesionales sanitarios es esencial para la confianza y la seguridad y el uso adecuado de los datos de salud y, por ende, lograr una aplicación satisfactoria del presente Reglamento. Los profesionales sanitarios se enfrentan a cambios profundos en el contexto de la digitalización y se les va a ofrecer más herramientas digitales como parte de la aplicación del EEDS. Por ello, necesitan mejorar su alfabetización sanitaria digital y sus competencias digitales y los Estados miembros deben proporcionar el acceso a los profesionales sanitarios a cursos de capacitación digital con el fin de que puedan prepararse para trabajar con sistemas HCE. Gracias a estos cursos, los profesionales sanitarios y los técnicos informáticos deben estar suficientemente formados para trabajar con las nuevas infraestructuras digitales, a fin de garantizar la ciberseguridad y la gestión ética de los datos de salud. Los cursos de formación deben elaborarse, revisarse y actualizarse periódicamente, en consulta y cooperación con los expertos pertinentes. Asimismo, la mejora de la alfabetización sanitaria digital es fundamental para facultar a las personas físicas para que ejerzan un verdadero control sobre sus datos de salud, gestionen activamente su salud y su asistencia, y entiendan las implicaciones de la gestión de tales datos para un uso tanto primario como secundario. Los diferentes grupos demográficos tienen distintos grados de alfabetización digital, lo que puede afectar a la capacidad de las personas físicas para ejercer los derechos de control de sus datos de salud electrónicos. Por consiguiente, los Estados miembros, incluidas las autoridades regionales y locales, deben apoyar la alfabetización sanitaria digital y la concienciación de la ciudadanía, velando al mismo tiempo por que la aplicación del presente Reglamento contribuya a reducir las desigualdades y no discrimine a las personas que carecen de capacidades digitales. Debe prestarse especial atención a las personas con discapacidad y a los grupos vulnerables, incluidas las personas migrantes y las de edad avanzada. Los Estados miembros deben crear programas nacionales específicos de alfabetización digital, incluidos programas para maximizar la inclusión social y garantizar que todas las personas físicas puedan ejercer eficazmente sus derechos en virtud del presente Reglamento. Los Estados miembros también deben ofrecer orientaciones centradas en el paciente a las personas físicas en relación con el uso de historias clínicas electrónicas y el uso primario de sus datos de salud electrónicos personales. Las orientaciones deben adaptarse al nivel de alfabetización sanitaria digital del paciente, prestando especial atención a las necesidades de los grupos vulnerables.

(90) También se debe utilizar financiación para contribuir al logro de los objetivos del EEDS. Al definir las condiciones para la contratación pública, las convocatorias de propuestas y la asignación de fondos de la Unión, incluidos los Fondos Estructurales y de Cohesión, los compradores públicos, las autoridades nacionales competentes de los Estados miembros, incluidas las autoridades de salud digital y los organismos de acceso a datos de salud, y la

Comisión, deben hacer referencia a las especificaciones técnicas, las normas y los perfiles aplicables en materia de interoperabilidad, seguridad y calidad de los datos, así como a otros requisitos desarrollados en virtud del presente Reglamento. Es necesario distribuir los fondos de la Unión de manera transparente entre los Estados miembros, teniendo en cuenta los diferentes niveles de digitalización de los sistemas sanitarios. La puesta a disposición de los datos para uso secundario requiere recursos adicionales para los sistemas de asistencia sanitaria, en particular los sistemas públicos de asistencia sanitaria. Esa carga adicional debe abordarse y minimizarse durante la fase de aplicación del EEDS.

(91) La aplicación del EEDS requiere inversiones adecuadas en el desarrollo de capacidades y en la formación, así como un compromiso bien financiado con la consulta y la participación públicas a escala de la Unión y nacional. Los costes económicos de la aplicación del presente Reglamento van a necesitar ser sufragados tanto a nivel de la Unión como nacional, y debe encontrarse un reparto equitativo de esa carga entre los fondos de la Unión y los nacionales.

(92) Determinadas categorías de datos de salud electrónicos pueden seguir siendo especialmente sensibles incluso cuando estén en formato anonimizado y, por tanto, no sean personales, como ya se prevé específicamente en el Reglamento (UE) 2022/868. Incluso cuando se utilizan técnicas de anonimización de última generación, sigue existiendo un riesgo residual de que la capacidad de reidentificación pueda estar disponible o se vuelva disponible, más allá de los medios cuya utilización sea razonablemente previsible. Ese riesgo residual está presente en relación con las enfermedades raras, a saber, afecciones potencialmente mortales o debilitantes crónicas que no afectan a más de cinco de cada diez mil personas en la Unión, en las que el número limitado de casos reduce la posibilidad de agregar plenamente los datos publicados con el fin de preservar la privacidad de las personas físicas, y mantener al mismo tiempo un nivel adecuado de granularidad para que los datos sigan siendo significativos. Tal riesgo residual puede afectar a diferentes categorías de datos de salud y puede conducir a la reidentificación de los interesados utilizando medios que vayan más allá de aquellos cuya utilización sea razonablemente previsible. Tal riesgo depende del nivel de granularidad, de la descripción de las características de los interesados, del número de personas afectadas, por ejemplo, en casos de datos incluidos en historias clínicas electrónicas, registros de enfermedades, biobancos y datos generados por personas, en los que la gama de características de identificación es más amplia, y también depende de la posible combinación con otra información, por ejemplo, en zonas geográficas muy pequeñas, o a través de la utilización de métodos tecnológicos que no estaban disponibles en el momento de la anonimización. Tal reidentificación de las personas físicas sería motivo de gran preocupación y podría poner en riesgo la aceptación de las disposiciones sobre uso secundario previstas en el presente Reglamento. Además, las técnicas de agregación están menos probadas para los datos no personales que contienen, por ejemplo, secretos comerciales, como es el caso de la notificación de los ensayos clínicos y las investigaciones clínicas, y perseguir las infracciones de los secretos comerciales fuera de la Unión es más difícil en ausencia de una norma de protección internacional suficiente. Por lo tanto, en el caso de esas categorías de datos de salud, sigue existiendo un riesgo de reidentificación tras la anonimización o agregación, que no puede atenuarse razonablemente en un principio. Esto se ajusta a los criterios indicados en el artículo 5, apartado 13, del Reglamento (UE) 2022/868. Esas categorías de datos de salud forman parte de la facultad para la transferencia a terceros países, establecida en el artículo 5, apartado 13, de dicho Reglamento. Las condiciones especiales establecidas en la delegación de poderes prevista en el artículo 5, apartado 13, del Reglamento (UE) 2022/868 se detallarán en el contexto del acto delegado en virtud de esa delegación de poderes y han de ser proporcionales al riesgo de reidentificación y tener en cuenta las especificidades de las diferentes categorías de datos o de las diferentes técnicas de anonimización o agregación.

(93) El tratamiento de grandes cantidades de datos de salud electrónicos personales a efectos del EEDS como parte de las actividades de tratamiento de datos en el contexto de la tramitación de solicitudes de acceso a datos de salud, permisos de datos y peticiones de datos de salud conlleva mayores riesgos de acceso no autorizado a dichos datos personales, así como la posibilidad de incidentes de ciberseguridad. Los datos de salud electrónicos personales son especialmente sensibles, ya que a menudo contienen información amparada por el secreto médico cuya divulgación a terceros no autorizados puede causar un notable trastorno. Teniendo plenamente en cuenta los principios expuestos en la jurisprudencia del Tribunal de Justicia de la Unión Europea, el presente Reglamento garantiza el pleno respeto de los derechos fundamentales, del derecho a la intimidad y del principio de proporcionalidad. Con el fin de asegurar la plena integridad y confidencialidad de los datos de salud electrónicos personales en virtud del presente Reglamento, garantizar un nivel especialmente elevado de protección y seguridad y reducir el riesgo de acceso ilícito a dichos datos de salud electrónicos personales, el presente Reglamento permite a los Estados miembros exigir que los datos de salud electrónicos personales se almacenen y traten únicamente en la Unión a efectos de las funciones previstas en él, a menos que sea de aplicación una decisión de adecuación adoptada con arreglo al artículo 45 del Reglamento (UE) 2016/679.

(94) El acceso a datos de salud electrónicos por parte de usuarios de datos de salud establecidos en terceros países o por organizaciones internacionales debe producirse únicamente con arreglo al principio de reciprocidad. Poner datos de salud electrónicos a disposición de un tercer país debe permitirse únicamente cuando la Comisión haya establecido, mediante un acto de ejecución, que el tercer país en cuestión permite el acceso a datos de salud electrónicos procedentes de dicho tercer país por entidades de la Unión con arreglo a las mismas condiciones y con las mismas salvaguardias que entidades accediesen a datos de salud electrónicos en la Unión. La Comisión debe hacer un

seguimiento y realizar una revisión periódica de la situación en esos terceros países y respecto de las organizaciones internacionales, y elaborar una lista de esos actos de ejecución. Cuando la Comisión considere que un tercer país ya no garantiza el acceso en las mismas condiciones, debe revocar el acto de ejecución correspondiente.

(95) Con el fin de promover la aplicación coherente del presente Reglamento, incluida la interoperabilidad transfronteriza de los datos de salud electrónicos, debe crearse un Consejo del Espacio Europeo de Datos de Salud. La Comisión debe participar en sus actividades y copresidirlo. El Consejo del EEDS debe poder emitir contribuciones escritas relacionadas con la aplicación coherente del presente Reglamento en toda la Unión, también prestando ayuda a los Estados miembros a coordinar el uso de datos de salud electrónicos para la asistencia sanitaria y la certificación, así como en relación con el uso secundario, y la financiación de esas actividades. Esto también puede incluir el intercambio de información sobre riesgos e incidentes en entornos de tratamiento seguros. El intercambio de este tipo de información no afecta a las obligaciones derivadas de otros actos jurídicos, como las notificaciones de violación de la seguridad de los datos en virtud del Reglamento (UE) 2016/679. En términos más generales, las actividades del Consejo del EEDS se entienden sin perjuicio de las facultades de las autoridades de control de conformidad con el Reglamento (UE) 2016/679. Dado que, a nivel nacional, las autoridades de salud digital que se ocupan del uso primario pueden ser diferentes de los organismos de acceso a datos de salud que se ocupan del uso secundario, las funciones son diferentes y es necesaria una cooperación distinta en cada uno de esos ámbitos, el Consejo del EEDS debe poder crear subgrupos que se ocupen de esas dos funciones, así como otros subgrupos, en caso necesario. En aras de un método de trabajo eficiente, las autoridades de salud digital y los organismos de acceso a datos de salud deben crear redes y vínculos a nivel nacional con otros organismos y autoridades, pero también a escala de la Unión. Dichos organismos podrían ser las autoridades de protección de datos, organismos de ciberseguridad, identificación electrónica y normalización, así como los organismos y grupos de expertos en virtud de los Reglamentos (UE) 2022/868, (UE) 2023/2854, (UE) 2024/1689 y el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([21]). El Consejo del EEDS debe funcionar de manera independiente, en aras del interés público y de conformidad con su código de conducta.

(96) Cuando se debatan cuestiones consideradas de particular importancia según el Consejo del EEDS, este debe poder invitar a observadores, como el SEPD, representantes de las instituciones de la Unión, incluido el Parlamento Europeo, y otras partes interesadas.

(97) Debe crearse un foro de partes interesadas con el fin de asesorar al Consejo del EEDS en el desempeño de sus funciones mediante aportaciones de las partes interesadas en asuntos relacionados con el presente Reglamento. El foro de partes interesadas debe estar integrado, entre otros, por representantes de organizaciones de pacientes y de consumidores, profesionales sanitarios, sector empresarial, investigadores científicos y el mundo académico. Debe tener una composición equilibrada y representar los puntos de vista de las diferentes partes interesadas pertinentes. Deben estar representados tanto los intereses comerciales como los no comerciales.

(98) Con el fin de garantizar una gestión cotidiana adecuada de las infraestructuras transfronterizas para el uso primario y el uso secundario, es necesario crear grupos rectores compuestos por representantes de los Estados miembros. Estos grupos rectores deben tomar decisiones operativas sobre la gestión técnica cotidiana de las infraestructuras transfronterizas y su desarrollo técnico, por ejemplo, sobre los cambios técnicos de las infraestructuras, la mejora de las funcionalidades o los servicios, o la garantía de la interoperabilidad con otras infraestructuras, sistemas digitales o espacios de datos. Sus actividades no deben incluir contribuir a la elaboración de actos de ejecución que afecten a esas infraestructuras. Esos grupos rectores también deben poder invitar a sus reuniones a representantes de otros participantes autorizados en DatosSalud@UE en calidad de observadores y deben consultar a los expertos pertinentes en el desempeño de sus funciones.

(99) Sin perjuicio de cualquier otro recurso administrativo, judicial o extrajudicial, toda persona física o jurídica debe tener derecho a presentar una reclamación ante una autoridad de salud digital o ante un organismo de acceso a datos de salud cuando considere que sus derechos o intereses en virtud del presente Reglamento se han visto afectados. La investigación abierta a raíz de una reclamación debe llevarse a cabo, bajo control judicial, según convenga en el caso específico. La autoridad de salud digital u organismo de acceso a datos de salud debe informar a la persona física o jurídica de los avances y el resultado de la reclamación en un plazo razonable. Si el caso requiere más investigación o coordinación con otra autoridad de salud digital u organismo de acceso a datos de salud, debe darse información sobre el estado de tramitación de las reclamaciones a la persona física o jurídica. A fin de facilitar la presentación de reclamaciones, cada autoridad de salud digital y organismo de acceso a datos de salud debe adoptar medidas, como proporcionar un formulario de presentación de reclamaciones que también pueda cumplimentarse electró-

([21]) Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 (Reglamento sobre la Ciberseguridad) (DO L 151 de 7.6.2019, p. 15).

nicamente, sin excluir la posibilidad de utilizar otros medios de comunicación. Cuando la reclamación se refiera a los derechos de las personas físicas en relación con la protección de sus datos personales, la autoridad de salud digital o el organismo de acceso a datos de salud transmitirán la reclamación a las autoridades de control de conformidad con el Reglamento (UE) 2016/679. Las autoridades de salud digital o los organismos de acceso a datos de salud deben cooperar para tramitar y resolver sin demora indebida las reclamaciones, lo que incluye el intercambio de toda información pertinente por medios electrónicos.

(100) La persona física que considere que se han vulnerado los derechos que le reconoce el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro constituida con arreglo al Derecho nacional, que tenga objetivos legales de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación.

(101) La autoridad de salud digital, el organismo de acceso a datos de salud, el tenedor de datos de salud o el usuario de datos de salud debe indemnizar cualesquiera daños y perjuicios que sufra una persona física o jurídica como consecuencia de una infracción del presente Reglamento. El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia de la Unión Europea, de tal modo que se respeten plenamente los objetivos del presente Reglamento. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras disposiciones del Derecho de la Unión o nacional. Las personas físicas deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos.

(102) A fin de reforzar la aplicación de lo dispuesto en el presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a las medidas adecuadas impuestas por los organismos de acceso a datos de salud en virtud del presente Reglamento, o en sustitución de estas. La imposición de sanciones, incluidas las multas administrativas, debe respetar las garantías procesales adecuadas conforme a los principios generales del Derecho de la Unión y de la Carta de los Derechos Fundamentales de la Unión Europea, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(103) Procede establecer disposiciones que permitan a los organismos de acceso a datos de salud aplicar multas administrativas por determinadas infracciones del presente Reglamento, que deban considerarse en el marco del presente Reglamento infracciones graves como la reidentificación de personas físicas, la descarga de datos de salud electrónicos personales fuera del entorno de tratamiento seguro o el tratamiento de datos para usos prohibidos o usos que no entren en el ámbito de un permiso de datos. El presente Reglamento debe detallar dichas infracciones, así como el límite máximo y los criterios para fijar las correspondientes multas administrativas, que debe determinar en cada caso concreto el organismo de acceso a datos de salud competente teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o atenuar las consecuencias de la infracción. A efectos de la imposición de multas administrativas en virtud del presente Reglamento, el concepto de empresa debe entenderse con arreglo a los artículos 101 y 102 del TFUE. Debe corresponder a los Estados miembros determinar si cabe imponer multas administrativas a las autoridades públicas, y en qué medida. La imposición de una multa administrativa o la formulación de una advertencia no debe afectar al ejercicio de otras potestades de los organismos de acceso a datos de salud ni a la aplicación de otras sanciones al amparo del presente Reglamento.

(104) A fin de garantizar que el EEDS cumple sus objetivos, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE por lo que respecta a la modificación o supresión en el anexo I de las categorías prioritarias de datos de salud electrónicos personales, la lista de datos obligatorios que han de registrar los fabricantes de sistemas HCE y de aplicaciones de bienestar en la base de dato de la UE para el registro de sistemas HCE y aplicaciones de bienestar, así como las modificaciones, adiciones o supresiones de elementos que deban formar parte de la etiqueta de calidad y utilidad de los datos. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación ([22]). En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(105) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución en lo que respecta a:

— las especificaciones técnicas para la interoperabilidad de los servicios de representación de los Estados miembros,

([22]) DO L 123 de 12.5.2016, p. 1.

— los requisitos para la calidad de los datos para el registro de datos de salud electrónicos personales en un sistema HCE,

— especificaciones transfronterizas para categorías de datos de salud electrónicos personales,

— las categorías prioritarias de datos de salud electrónicos personales, estableciendo el formato europeo de intercambio de historias clínicas electrónicas,

— actualizaciones sobre el formato europeo de intercambio de historias clínicas electrónicas para integrar las revisiones pertinentes de los sistemas y nomenclaturas de codificación de la asistencia sanitaria,

— especificaciones técnicas que amplíen el formato europeo de intercambio de historias clínicas electrónicas a las categorías adicionales de datos de salud electrónicos personales,

— los requisitos para el mecanismo interoperable y transfronterizo de identificación y autenticación para las personas físicas y los profesionales sanitarios, de conformidad con el Reglamento (UE) n.º 910/2014,

— los requisitos para la ejecución técnica de los derechos de las personas físicas en relación con el uso primario de sus datos de salud electrónicos personales,

— las medidas necesarias para el desarrollo técnico de MiSalud@UE, disposiciones pormenorizadas relativas a la seguridad, la confidencialidad y la protección de los datos de salud electrónicos personales, así como las condiciones para las comprobaciones del cumplimiento necesarias para unirse y permanecer conectado a MiSalud@UE,

— disposiciones sobre los requisitos de ciberseguridad, interoperabilidad técnica, interoperabilidad semántica, operaciones y gestión de servicios en relación con el tratamiento por parte de la Comisión y sus responsabilidades con respecto a los responsables del tratamiento,

— los aspectos técnicos de los servicios complementarios prestados a través de MiSalud@UE,

— los aspectos técnicos de los intercambios de datos de salud electrónicos personales entre MiSalud@UE y otros servicios o infraestructuras,

— la conexión de otras infraestructuras, de puntos de contacto nacionales para la salud digital de terceros países o sistemas establecidos a nivel internacional por organizaciones internacionales a la plataforma de MiSalud@UE y su desconexión de esta,

— especificaciones comunes con respecto a los requisitos esenciales establecidos en el anexo II,

— especificaciones comunes para el entorno digital de pruebas europeo,

— justificaciones de las medidas nacionales adoptadas por las autoridades de vigilancia del mercado, en caso de incumplimiento de sistemas HCE,

— el formato y el contenido de la etiqueta de las aplicaciones de bienestar,

— los principios para las políticas y las estructuras de las tasas que los organismos de acceso a datos de salud y los tenedores fiables de datos de salud pueden cobrar por la puesta a disposición de datos de salud electrónicos para uso secundario,

— la arquitectura de una herramienta informática destinada a apoyar y hacer transparente para los organismos de acceso a datos de salud las medidas de garantía del cumplimiento,

— el logotipo para hacer patente la contribución del EEDS,

— modelos de la solicitud de acceso a datos de salud, del permiso de datos y de la petición de datos de salud,

— los requisitos técnicos, organizativos, de seguridad de la información, de confidencialidad, de protección de datos y de interoperabilidad para los entornos de tratamiento seguros,

— modelos para los acuerdos entre responsables del tratamiento y encargados del tratamiento,

— decisiones sobre el cumplimiento de un punto de contacto nacional para uso secundario de un tercer país o de un sistema establecido a nivel internacional por organizaciones internacionales de los requisitos de DatosSalud@UE a efectos del uso secundario de datos de salud, sobre el cumplimiento del capítulo IV del presente Reglamento y sobre si dicho punto de contacto nacional para uso secundario de un tercer país o dicho sistema da acceso a usuarios de datos de salud situados en la Unión a los datos de salud electrónicos a los que tiene acceso en condiciones equivalentes,

— los requisitos, las especificaciones técnicas y la arquitectura informática de DatosSalud@UE; las condiciones y comprobaciones del cumplimiento para unirse y permanecer conectado a DatosSalud@UE; los criterios mínimos que deben cumplir los puntos de contacto nacionales para uso secundario y los participantes autorizados en DatosSalud@UE; las responsabilidades de los responsables del tratamiento y de los encargados del tratamiento que participen en DatosSalud@UE; las responsabilidades de los responsables y de los encargados del tratamiento en relación con el entorno de tratamiento seguro gestionado por la Comisión, y las especificaciones comunes para la arquitectura de DatosSalud@UE y para su interoperabilidad con otros espacios comunes europeos de datos,

— las decisiones de conexión de participantes autorizados concretos a DatosSalud@UE,

— los elementos mínimos para los conjuntos de datos y las características de esos elementos que deben proporcionar los tenedores de datos de salud,

— las características visuales y las especificaciones técnicas de la etiqueta de calidad y utilidad de los datos,

— las especificaciones mínimas de los conjuntos de datos de alto impacto para el uso secundario

— decisiones sobre si un tercer país permite que los solicitantes de datos de salud de la Unión accedan a los datos de salud electrónicos en dicho tercer país en condiciones que no sean más restrictivas que las establecidas en el presente Reglamento,

— las medidas necesarias para el establecimiento y la actividad del Consejo del EEDS.

Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([23]).

(106) Los Estados miembros deben tomar todas las medidas necesarias para asegurarse de que se apliquen las disposiciones del presente Reglamento, también mediante el establecimiento de sanciones efectivas, proporcionadas y disuasorias para las infracciones que se cometan. A la hora de decidir la cuantía de la sanción para cada caso concreto, los Estados miembros deben tener en cuenta los límites y criterios establecidos en el presente Reglamento. La reidentificación de personas físicas debe considerarse una vulneración grave del presente Reglamento.

(107) La aplicación del EEDS va a necesitar un importante trabajo de desarrollo para los Estados miembros y los servicios centrales. Con el fin de hacer un seguimiento de los avances realizados a ese respecto, la Comisión debe, hasta la plena aplicación del presente Reglamento, informar anualmente sobre dichos avances, teniendo en cuenta la información proporcionada por los Estados miembros. Esos informes pueden incluir recomendaciones de medidas correctoras, así como una evaluación de los avances realizados.

(108) La Comisión debe efectuar una evaluación del presente Reglamento, a fin de valorar si este alcanza sus objetivos de manera eficaz y eficiente, es coherente y sigue siendo pertinente y aporta valor añadido a escala de la Unión. La Comisión debe efectuar una evaluación específica del presente Reglamento en un plazo de ocho años a partir de su entrada en vigor, y una evaluación global en un plazo de diez años a partir de su entrada en vigor. Tras cada evaluación, la Comisión debe presentar informes sobre sus principales conclusiones al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.

(109) Para el éxito de la aplicación transfronteriza del EEDS, el Marco Europeo de Interoperabilidad, cuyo ámbito se puso al día y amplió mediante la Comunicación de la Comisión, de 23 de marzo de 2017, titulada «Marco Europeo de Interoperabilidad – Estrategia de aplicación» para tener en cuenta los nuevos o revisados requisitos de interoperabilidad, debe considerarse una referencia común para garantizar la interoperabilidad jurídica, organizativa, semántica y técnica.

(110) Dado que los objetivos del presente Reglamento, a saber, facultar a las personas físicas al proporcionarles un mayor control de sus datos de salud electrónicos personales y apoyar su libertad de circulación garantizando que sus datos de salud los acompañen, fomentar un auténtico mercado interior de servicios y productos sanitarios digitales, y garantizar un marco coherente y eficiente para la reutilización de los datos de salud de las personas físicas con fines de investigación, innovación, formulación de políticas y actividades de regulación, no pueden ser alcanzados de manera suficiente por los Estados miembros únicamente mediante medidas de coordinación, como demuestra la

([23]) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

evaluación de los aspectos digitales de la Directiva 2011/24/UE, sino que, debido a que las medidas de armonización relativas a los derechos de las personas físicas en relación con sus datos de salud electrónicos, la interoperabilidad de los datos de salud electrónicos y un marco común y garantías para el uso primario y secundario, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos.

(111) La evaluación de los aspectos digitales de la Directiva 2011/24/UE muestra que la eficacia de la red de sanidad electrónica es limitada, pero también que hay un gran potencial para trabajar a nivel de la Unión en el ámbito de la salud digital, como se ha demostrado por el trabajo efectuado durante la pandemia de COVID-19. Por lo tanto, procede modificar la Directiva 2011/24/UE en consecuencia.

(112) El presente Reglamento complementa los requisitos esenciales de ciberseguridad establecidos en el Reglamento (UE) 2024/2847. Los sistemas HCE que sean productos con elementos digitales en el sentido del Reglamento (UE) 2024/2847 también deben cumplir los requisitos esenciales de ciberseguridad establecidos en dicho Reglamento. Los fabricantes de dichos sistemas HCE deben demostrar la conformidad con arreglo a lo dispuesto en el presente Reglamento. A fin de facilitar dicha conformidad, los fabricantes deben poder elaborar un único conjunto de documentos técnicos que contenga los elementos exigidos por ambos actos jurídicos. Debe ser posible demostrar, a través del marco de evaluación en virtud del presente Reglamento, la conformidad de los sistemas HCE con los requisitos esenciales de ciberseguridad establecidos en el Reglamento (UE) 2024/2847. No obstante, no deben aplicarse las partes del procedimiento de evaluación de la conformidad en el marco del presente Reglamento relacionadas con la utilización de entornos de pruebas ya que dichos entornos de pruebas no permiten una evaluación de la conformidad con respecto a los requisitos esenciales de ciberseguridad. Dado que el Reglamento (UE) 2024/2847 no se aplica directamente al software como servicio (SaaS) como tal, los sistemas HCE que se ofrecen a través de una licencia SaaS y los modelos de prestación no entran en el ámbito de aplicación del presente Reglamento. Del mismo modo, los sistemas HCE que se desarrollen y utilicen en interno no entran en el ámbito de aplicación del presente Reglamento, puesto que no se introducen en el mercado.

(113) El SEPD y el CEPD, a los que se consultó de conformidad con el artículo 42, apartados 1 y 2, del Reglamento (UE) 2018/1725, emitieron su dictamen conjunto el 12 de julio de 2022.

(114) El presente Reglamento no debe afectar a la aplicación de la normativa sobre competencia, en particular los artículos 101 y 102 del TFUE. Las disposiciones del presente Reglamento no deben utilizarse para restringir la competencia de forma contraria al TFUE.

(115) Dada la necesidad de preparación técnica, el presente Reglamento debe ser aplicable a partir del 26 de marzo de 2027. Con el fin de contribuir a la ejecución satisfactoria del EEDS y a la creación de condiciones favorables para la cooperación europea en materia de datos de salud, la ejecución debe realizarse por etapas.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. El presente Reglamento establece el Espacio Europeo de Datos de Salud (EEDS), para lo cual se disponen reglas, normas e infraestructuras comunes y un marco de gobernanza, con vistas a facilitar el acceso a los datos de salud electrónicos a efectos del uso primario de los datos de salud electrónicos y el uso secundario de estos datos.

2. El presente Reglamento:

a) desarrolla y complementa los derechos de las personas físicas establecidos en el Reglamento (UE) 2016/679 con respecto al uso primario y uso secundario de sus datos de salud electrónicos personales;

b) establece reglas comunes para los sistemas de historias clínicas electrónicas («sistemas HCE») en relación con dos componentes obligatorios armonizados de programa informático, a saber, el componente de programa informático europeo de interoperabilidad para sistemas HCE y el componente de programa informático europeo de registro para sistemas HCE, tal como se definen en el artículo 2, apartado 2, letras n) y o), respectivamente, y para las aplicaciones de

bienestar para las que se afirme que son interoperables con los sistemas HCE en relación con esos dos componentes armonizados de programa informático, en lo que respecta al uso primario de datos de salud electrónicos;

c) introduce reglas y mecanismos comunes para el uso primario y el uso secundario de datos de salud electrónicos;

d) establece una infraestructura transfronteriza que permitirá el uso primario de datos de salud electrónicos personales en el conjunto de la Unión;

e) establece una infraestructura transfronteriza para el uso secundario de datos de salud electrónicos;

f) establece mecanismos de gobernanza y coordinación a nivel de la Unión y nacional tanto para el uso primario como para el uso secundario de datos de salud electrónicos.

3. El presente Reglamento se entenderá sin perjuicio de otros actos jurídicos de la Unión relativos al acceso a los datos de salud electrónicos, al intercambio o al uso secundario de estos, o a los requisitos de la Unión relativos al tratamiento de datos en lo que respecta a los datos de salud electrónicos, en particular los Reglamentos (CE) n.º 223/2009 ([24]), (UE) n.º 536/2014 ([25]), (UE) 2016/679, (UE) 2018/1725, (UE) 2022/868 y (UE) 2023/2854 del Parlamento Europeo y del Consejo, y las Directivas 2002/58/CE ([26]) y (UE) 2016/943 ([27]) del Parlamento Europeo y del Consejo.

4. Las referencias en el presente Reglamento a las disposiciones del Reglamento (UE) 2016/679 se entenderán también como referencias a las disposiciones correspondientes del Reglamento (UE) 2018/1725, cuando proceda, por lo que respecta a las instituciones, órganos y organismos de la Unión.

5. El presente Reglamento se entenderá sin perjuicio de los Reglamentos (UE) 2017/745, (UE) 2017/746 y (UE) 2024/1689, en lo que respecta a la seguridad de los productos sanitarios, los productos sanitarios para diagnóstico *in vitro* y los sistemas de inteligencia artificial (IA) que interactúan con los sistemas HCE.

6. El presente Reglamento se entenderá sin perjuicio del Derecho de la Unión o nacional respecto del tratamiento de datos de salud electrónicos a efectos de la presentación de informes, la respuesta a las peticiones de acceso a la información o la demostración o verificación del cumplimiento de las obligaciones legales, o del Derecho de la Unión o nacional en relación con la concesión de acceso a documentos oficiales y su divulgación.

7. El presente Reglamento se entenderá sin perjuicio de las disposiciones específicas del Derecho de la Unión o nacional que prevean el acceso a datos de salud electrónicos para su posterior tratamiento por parte de organismos del sector público de los Estados miembros, de las instituciones, órganos y organismos de la Unión, o de entidades privadas a las que el Derecho de la Unión o nacional haya encomendado una misión de interés público, con el fin de desempeñar dicha misión.

8. El presente Reglamento no afectará al acceso a datos de salud electrónicos para uso secundario convenido en el marco de acuerdos contractuales o administrativos entre entidades públicas o privadas.

9. El presente Reglamento no se aplicará al tratamiento de datos personales en los casos siguientes:

a) cuando el tratamiento se realice en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) cuando el tratamiento se realice por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

([24]) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008, relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo, sobre la estadística comunitaria, y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164).

([25]) Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (DO L 158 de 27.5.2014, p. 1).

([26]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

([27]) Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DO L 157 de 15.6.2016, p. 1).

Artículo 2

Definiciones

1. A los efectos del presente Reglamento, se aplicarán las definiciones siguientes:

a) las definiciones de «datos personales», «tratamiento», «seudonimización», «responsable del tratamiento», «encargado del tratamiento», «tercero», «consentimiento del interesado», «datos genéticos», «datos relativos a la salud» y «organización internacional» establecidas en el artículo 4, puntos 1, 2, 5, 7, 8, 10, 11, 13, 15 y 26, respectivamente, del Reglamento (UE) 2016/679;

b) las definiciones de «asistencia sanitaria», «Estado miembro de afiliación», «Estado miembro de tratamiento», «profesional sanitario», «prestador de asistencia sanitaria», «medicamento» y «receta» establecidas en el artículo 3, letras a), c), d), f), g), i) y k), respectivamente, de la Directiva 2011/24/UE;

c) las definiciones de «datos», «acceso», «cesión altruista de datos», «organismo del sector público» y «entorno de tratamiento seguro» establecidas en el artículo 2, puntos 1, 13, 16, 17 y 20, respectivamente, del Reglamento (UE) 2022/868;

d) las definiciones de «comercialización», «introducción en el mercado», «vigilancia del mercado», «autoridad de vigilancia del mercado», «incumplimiento», «fabricante», «importador», «distribuidor», «operador económico», «medida correctiva», «recuperación» y «retirada» establecidas en el artículo 3, puntos 1, 2, 3, 4, 7, 8, 9, 10, 13, 16, 22 y 23, respectivamente, del Reglamento (UE) 2019/1020;

e) las definiciones de «producto sanitario», «finalidad prevista», «instrucciones de uso», «funcionamiento de un producto», «centro sanitario» y «especificaciones comunes» establecidas en el artículo 2, puntos 1, 12, 14, 22, 36 y 71, respectivamente, del Reglamento (UE) 2017/745;

f) las definiciones de «identificación electrónica» y «medios de identificación electrónica» establecidas en el artículo 3, puntos 1 y 2, respectivamente, del Reglamento (UE) n.º 910/2014;

g) la definición de «poderes adjudicadores» establecida en el artículo 2, apartado 1, punto 1, de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo ([28]);

h) la definición de «salud pública» establecida en el artículo 3, letra c), del Reglamento (UE) n.º 1338/2008 del Parlamento Europeo y del Consejo ([29]).

2. Además, a los efectos del presente Reglamento, se entenderá por:

a) «datos de salud electrónicos personales»: los datos relativos a la salud y los datos genéticos, que se traten en formato electrónico;

b) «datos de salud electrónicos no personales»: los datos de salud electrónicos distintos de los datos de salud electrónicos personales, que incluyen tanto los datos que han sido anonimizados de modo que ya no están relacionados con una persona física identificada o identificable (el «interesado»), como los datos que nunca han estado relacionados con un interesado;

c) «datos de salud electrónicos»: los datos de salud electrónicos personales o no personales;

d) «uso primario»: el tratamiento de datos de salud electrónicos para la prestación de asistencia sanitaria con el fin de evaluar, conservar o restablecer el estado de salud de la persona física a la que se refieren dichos datos, que incluye la receta, dispensación y provisión de medicamentos y productos sanitarios, así como para los servicios sociales, administrativos o de reembolso pertinentes;

e) «uso secundario»: el tratamiento de datos de salud electrónicos para los fines establecidos en el capítulo IV del presente Reglamento distintos de los fines iniciales para los que se recogieron o produjeron;

f) «interoperabilidad»: la capacidad de las organizaciones, así como de las aplicaciones informáticas o dispositivos procedentes del mismo fabricante o de diferentes fabricantes, para interactuar, a través de los procesos que admiten, que implique un intercambio de información y conocimientos, sin que modifique el contenido de los datos, entre esas organizaciones, aplicaciones informáticas o dispositivos;

([28]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

([29]) Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31.12.2008, p. 70).

g) «registro de datos de salud electrónicos»: el registro de datos de salud en un formato electrónico, mediante la introducción manual de tales datos, la recogida de tales datos con un dispositivo, o mediante la conversión de datos de salud no electrónicos a formato electrónico, para que puedan ser tratados en un sistema HCE o en una aplicación de bienestar;

h) «servicio de acceso a datos de salud electrónicos»: un servicio en línea, como un portal o una aplicación para dispositivos móviles, que permite a las personas físicas que no actúan en una condición de profesional acceder a sus propios datos de salud electrónicos o a los de aquellas personas físicas a cuyos datos de salud electrónicos están autorizados a acceder legalmente;

i) «servicio de acceso de los profesionales sanitarios»: un servicio, compatible con un sistema HCE, que permite a los profesionales sanitarios acceder a los datos de las personas físicas a las que están tratando;

j) «historia clínica electrónica» o «HCE»: una recopilación de datos de salud electrónicos relacionados con una persona física y recogidos en el sistema sanitario, tratados a efectos de la prestación de asistencia sanitaria;

k) «sistema de historia clínica electrónica» o «sistema HCE»: todo sistema en el que el programa informático, o una combinación del soporte físico y el programa informático de dicho sistema, permite almacenar, intermediar, exportar, importar, convertir, editar o visualizar datos de salud electrónicos personales pertenecientes a las categorías prioritarias de datos de salud electrónicos personales establecidas en virtud del presente Reglamento, y está destinado por el fabricante a ser utilizado por los prestadores de asistencia sanitaria cuando prestan asistencia al paciente o por los pacientes cuando acceden a sus datos de salud electrónicos;

l) «puesta en servicio»: la primera utilización en la Unión, de acuerdo con su finalidad prevista, de un sistema HCE regulado en el presente Reglamento;

m) «componente de programa informático»: la parte separada de un programa informático que ofrece una funcionalidad específica o realiza funciones o procedimientos específicos y que puede funcionar de forma independiente o en combinación con otros componentes;

n) «componente de programa informático europeo de interoperabilidad para sistemas HCE»: un componente de programa informático del sistema HCE que proporciona y recibe los datos de salud electrónicos personales en la categoría prioritaria para uso primario establecida en virtud del presente Reglamento en el formato europeo de intercambio de historias clínicas electrónicas establecido en el presente Reglamento y que es independiente del componente de programa informático europeo de registro para sistemas HCE;

o) «componente de programa informático europeo de registro para sistemas HCE»: un componente de programa informático del sistema HCE que proporciona información de registro relativa al acceso de los profesionales sanitarios o de otras personas a las categorías prioritarias de los datos de salud electrónicos personales establecidas en virtud del presente Reglamento, en el formato definido en su anexo II, punto 3.2, y que es independiente del componente de programa informático europeo de interoperabilidad para sistemas HCE;

p) «marcado CE de conformidad»: un marcado por el que el fabricante indica que el sistema HCE es conforme con los requisitos aplicables establecidos en el presente Reglamento y con otras disposiciones aplicables del Derecho de la Unión que regulen su colocación en virtud del Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([30]);

q) «riesgo»: la combinación de la probabilidad de que se produzca un peligro que cause daños a la salud, la seguridad o la seguridad de la información con el nivel de gravedad de dicho daño;

r) «incidente grave»: todo funcionamiento defectuoso o deterioro de las características o del funcionamiento de un sistema HCE comercializado que, directa o indirectamente, dé lugar, pueda haber dado lugar o pueda dar lugar, a alguna de las siguientes consecuencias:

   i) la muerte de una persona física o el daño grave para su salud,

   ii) el perjuicio grave para los derechos de una persona física,

   iii) la perturbación grave de la gestión y la explotación de infraestructuras críticas en el sector sanitario;

([30]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

s) «asistencia»: un servicio profesional destinado a atender las necesidades específicas de una persona física que, debido a una discapacidad u otras condiciones físicas o mentales, necesita asistencia, incluidas medidas preventivas y de apoyo, para realizar actividades esenciales de la vida cotidiana con el fin de apoyar su autonomía personal;

t) «tenedor de datos de salud»: toda persona física o jurídica, autoridad pública, agencia u otro organismo del sector de la asistencia sanitaria o el asistencial, incluidos los servicios de reembolso cuando sea necesario, así como cualquier persona física o jurídica que desarrolle productos o servicios destinados al sector de la salud, el de la asistencia sanitaria o el asistencial, que desarrolle o cree aplicaciones de bienestar, que efectúe investigaciones científicas relacionadas con el sector de la asistencia sanitaria o el asistencial o que actúe como registro de mortalidad, así como las instituciones, órganos u organismos de la Unión, que tengan bien:

i) el derecho o la obligación, de conformidad con el Derecho de la Unión o nacional aplicable y en su calidad de responsable o corresponsable del tratamiento, de tratar datos de salud electrónicos personales para fines de prestación de asistencia sanitaria o fines asistenciales, o para fines de salud pública, reembolso, investigación, innovación, formulación de políticas, estadísticas oficiales o seguridad del paciente o para fines de regulación, o

ii) la capacidad de poner a disposición datos de salud electrónicos no personales mediante el control del diseño técnico de un producto y de los servicios conexos, incluido mediante el registro, la entrega, la limitación del acceso o el intercambio de dichos datos;

u) «usuario de datos de salud»: una persona física o jurídica, incluidas las instituciones, órganos u organismos de la Unión, a la que se ha concedido acceso lícito a datos de salud electrónicos para uso secundario en virtud de un permiso de datos, una petición de datos de salud o una aprobación de acceso por parte de un participante autorizado en DatosSalud@UE;

v) «permiso de datos»: una decisión administrativa expedida a un usuario de datos de salud por un organismo de acceso a datos de salud con el fin de que trate, para un uso secundario específico, determinados datos de salud electrónicos especificados en el permiso de datos en las condiciones establecidas en el capítulo IV del presente Reglamento;

w) «conjunto de datos»: una colección estructurada de datos de salud electrónicos;

x) «conjunto de datos de alto impacto para uso secundario»: un conjunto de datos cuya reutilización está asociada a beneficios significativos debido a su pertinencia para la investigación en el campo de la salud;

y) «catálogo de conjuntos de datos»: una colección de descripciones de conjuntos de datos, organizada de manera sistemática y que incluye una parte pública orientada al usuario, en la que se puede acceder a la información relativa a los parámetros individuales de los conjuntos de datos por medios electrónicos a través de un portal en línea;

z) «calidad de los datos»: el grado en que los elementos de los datos de salud electrónicos son adecuados para su uso primario previsto y su uso secundario previsto;

aa) «etiqueta de calidad y utilidad de los datos»: un diagrama gráfico, incluida una escala, que describe la calidad de los datos y las condiciones de uso de un conjunto de datos;

ab) «aplicación de bienestar»: todo programa informático, o toda combinación de soporte físico y programa informático, destinado por el fabricante a ser utilizado por una persona física para el tratamiento de datos de salud electrónicos, con el fin específico de proporcionar información sobre la salud de las personas físicas, o sobre la prestación de asistencia con fines distintos a la prestación de asistencia sanitaria.

CAPÍTULO II

USO PRIMARIO

SECCIÓN 1

Derechos de las personas físicas en relación con el uso primario de sus datos de salud electrónicos personales y disposiciones conexas

Artículo 3

Derecho de las personas físicas a acceder a sus datos de salud electrónicos personales

1. Las personas físicas tendrán derecho a acceder, al menos, a los datos de salud electrónicos personales con los que guarden relación pertenecientes a las categorías prioritarias a que se refiere el artículo 14, y que sean tratados para la prestación de asistencia sanitaria a través de los servicios de acceso a datos de salud electrónicos a que se refiere el artículo 4. El acceso se proporcionará inmediatamente después de que los datos de salud electrónicos personales se hayan registrado en un sistema HCE, respetando al mismo tiempo la necesaria viabilidad tecnológica, y se proporcionará de forma gratuita y en un formato fácilmente legible, consolidado y accesible.

2. Las personas físicas, o sus representantes mencionados en el artículo 4, apartado 2, tendrán derecho a descargar de forma gratuita una copia electrónica de, al menos, los datos de salud electrónicos personales de las categorías prioritarias a que se refiere el artículo 14 relacionados con esas personas físicas, a través de los servicios de acceso a datos de salud electrónicos a que se refiere el artículo 4, en el formato europeo de intercambio de historias clínicas electrónicas a que se refiere el artículo 15.

3. De conformidad con el artículo 23 del Reglamento (UE) 2016/679, los Estados miembros podrán limitar el alcance de los derechos establecidos en los apartados 1 y 2 del presente artículo, en particular cuando dichas limitaciones sean necesarias para proteger a las personas físicas, en consideración de la seguridad de los pacientes y la ética, retrasando el acceso a sus datos de salud electrónicos personales durante un tiempo limitado hasta que un profesional sanitario pueda comunicar y explicar adecuadamente a las personas físicas de que se trate la información que pueda tener consecuencias importantes para su salud.

Artículo 4

Servicios de acceso a datos de salud electrónicos para personas físicas y sus representantes

1. Los Estados miembros garantizarán que se establezcan uno o varios servicios de acceso a datos de salud electrónicos a nivel nacional, regional o local, de modo que se permita a las personas físicas acceder a sus datos de salud electrónicos personales y ejercer sus derechos establecidos en los artículos 3 y 5 a 10. Dichos servicios de acceso a datos de salud electrónicos serán gratuitos para las personas físicas y sus representantes a los que se refiere el apartado 2 del presente artículo.

2. Los Estados miembros garantizarán que se establezcan uno o varios servicios de representación como funcionalidad de los servicios de acceso a los datos de salud electrónicos que permitan:

a) a las personas físicas autorizar a otras personas físicas de su elección el acceso a sus datos de salud electrónicos personales, o a parte de ellos, en su nombre durante un período determinado o indeterminado y, en caso necesario, únicamente para un fin específico, y gestionar dichas autorizaciones, y

b) a los representantes legales de las personas físicas acceder a los datos de salud electrónicos personales de dichas personas físicas cuyos asuntos administren, de conformidad con el Derecho nacional.

Los Estados miembros establecerán reglas relativas a las autorizaciones a que se refiere el párrafo primero, letra a), y a las acciones de los tutores y otros representantes legales.

3. Los servicios de representación a que se refiere el apartado 2 proporcionarán autorizaciones gratuitas de una manera transparente y fácilmente comprensible y por vía electrónica o en papel. Las personas físicas y sus representantes serán informados sobre sus derechos de autorización, incluido el modo de ejercer dichos derechos, y sobre el proceso de autorización.

Los servicios de representación ofrecerán un mecanismo de reclamación sencillo para las personas físicas.

4. Los servicios de representación a que se refiere el apartado 2 del presente artículo serán interoperables entre los Estados miembros. La Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas para la interoperabilidad de los servicios de representación de los Estados miembros. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

5. Los servicios de acceso a datos de salud electrónicos y los servicios de representación serán fácilmente accesibles para las personas con discapacidad, los colectivos vulnerables y las personas con baja alfabetización digital.

Artículo 5

Derecho de las personas físicas a introducir información en su propia HCE

Las personas físicas, o sus representantes mencionados en el artículo 4, apartado 2, tendrán derecho a introducir información en la HCE de esas personas físicas a través de los servicios de acceso a datos de salud electrónicos o las aplicaciones relacionadas con dichos servicios a que se refiere dicho artículo. Se deberá poder distinguir claramente si la información ha sido introducida por la persona física o por su representante. Las personas físicas, o sus representantes mencionados en el artículo 4, apartado 2, no podrán modificar directamente los datos de salud electrónicos introducidos por profesionales sanitarios.

Artículo 6

Derecho de las personas físicas a la rectificación

Los servicios de acceso a datos de salud electrónicos a que se refiere el artículo 4 permitirán a las personas físicas solicitar fácilmente en línea la rectificación de sus datos de salud electrónicos personales de conformidad con el artículo 16 del Reglamento (UE) 2016/679. Cuando proceda, el responsable del tratamiento verificará con el profesional sanitario correspondiente la exactitud de la información proporcionada en la solicitud.

Los Estados miembros también podrán permitir a las personas físicas ejercer en línea otros derechos con arreglo al capítulo III del Reglamento (UE) 2016/679 a través de los servicios de acceso a datos de salud electrónicos.

Artículo 7

Derecho de las personas físicas a la portabilidad de los datos

1. Las personas físicas tendrán derecho a permitir el acceso a la totalidad o parte de sus datos de salud electrónicos personales a un prestador de asistencia sanitaria o a solicitarle que los transmita a otro prestador de asistencia sanitaria de su elección, de forma inmediata, gratuita y sin obstáculos por parte del prestador de asistencia sanitaria o de los fabricantes de los sistemas utilizados por ese prestador de asistencia sanitaria.

2. Cuando los prestadores de asistencia sanitaria estén situados en diferentes Estados miembros, las personas físicas tendrán derecho a solicitar la transmisión de sus datos de salud electrónicos personales en el formato europeo de intercambio de historias clínicas electrónicas a que se refiere el artículo 15 a través de la infraestructura transfronteriza a que se refiere el artículo 23. El prestador de asistencia sanitaria que reciba dichos datos los aceptará y los podrá leer.

3. Las personas físicas tendrán derecho a solicitar a un prestador de asistencia sanitaria que transmita una parte de sus datos de salud electrónicos personales a un destinatario claramente identificado en el sector de la seguridad social o de los servicios de reembolso. Dicha transmisión se efectuará de forma inmediata, gratuita y sin obstáculos por parte del prestador de asistencia sanitaria o de los fabricantes de los sistemas utilizados por ese prestador de asistencia sanitaria, y será de un solo sentido.

4. Cuando las personas físicas se hayan descargado una copia electrónica de sus categorías prioritarias de datos de salud electrónicos personales de conformidad con el artículo 3, apartado 2, podrán transmitir dichos datos a los prestadores de asistencia sanitaria de su elección en el formato europeo de intercambio de historias clínicas electrónicas a que se refiere el artículo 15. El prestador de asistencia sanitaria que reciba dichos datos los aceptará y los podrá leer, según corresponda.

Artículo 8

Derecho a limitar el acceso

Las personas físicas tendrán derecho a limitar el acceso de los profesionales sanitarios y los prestadores de asistencia sanitaria a la totalidad o parte de sus datos de salud electrónicos personales a que se refiere el artículo 3.

Cuando se ejerza el derecho a que se refiere el párrafo primero, se informará a las personas físicas de que limitar el acceso podría afectar a la asistencia sanitaria que se les preste.

El hecho de que una persona física haya limitado el acceso en virtud del párrafo primero no será visible para los prestadores de asistencia sanitaria.

Los Estados miembros establecerán las reglas y garantías específicas relativas a dichos mecanismos de limitación.

Artículo 9

Derecho a obtener información sobre el acceso a los datos

1. Las personas físicas tendrán derecho a obtener información, también a través de notificaciones automáticas, sobre cualquier acceso a sus datos de salud electrónicos personales a través del servicio de acceso de los profesionales sanitarios obtenido en el contexto de la asistencia sanitaria, incluido el acceso proporcionado de conformidad con el artículo 11, apartado 5.

2. La información a que se refiere el apartado 1 se proporcionará, de forma gratuita y sin demora, a través de los servicios de acceso a datos de salud electrónicos y estará disponible durante al menos tres años a partir de la fecha de acceso a los datos. Esa información incluirá, al menos, lo siguiente:

a) información acerca del prestador de asistencia sanitaria o cualquier otra persona que haya accedido a los datos de salud electrónicos personales;

b) la fecha y hora de acceso;

c) los datos de salud electrónicos personales a los que se ha accedido.

3. Los Estados miembros podrán prever limitaciones al derecho a que se refiere el apartado 1 en circunstancias excepcionales, cuando existan indicios concretos de que la divulgación pondría en peligro los derechos o intereses vitales del profesional sanitario o la asistencia prestada a la persona física.

Artículo 10

Derecho de las personas físicas a la autoexclusión para el uso primario

1. El Derecho de los Estados miembros podrá disponer que las personas físicas tengan un derecho de autoexclusión relativo al acceso a sus datos de salud electrónicos personales registrados en un sistema HCE a través de los servicios de acceso a datos de salud electrónicos a que se refieren los artículos 4 y 12. En tales casos, los Estados miembros garantizarán que el ejercicio de dicho derecho sea reversible.

2. Cuando un Estado miembro prevea el derecho a que se refiere el apartado 1 del presente artículo, deberá establecer las reglas y garantías específicas relativas al mecanismo de autoexclusión. En particular, los Estados miembros podrán establecer que el prestador de asistencia sanitaria o el profesional sanitario pueda acceder a los datos de salud electrónicos personales en los casos en que el tratamiento de datos sea necesario para proteger los intereses vitales del interesado o de otra persona física a que se refiere el artículo 9, apartado 2, letra c), del Reglamento (UE) 2016/679, incluso si el paciente ha ejercido el derecho de autoexclusión para el uso primario.

Artículo 11

Acceso de los profesionales sanitarios a los datos de salud electrónicos personales

1. Cuando los profesionales sanitarios traten datos en formato electrónico, tendrán acceso a los datos de salud electrónicos personales pertinentes y necesarios de las personas físicas a las que estén tratando, a través de los servicios de acceso de los profesionales sanitarios a que se refiere el artículo 12, con independencia del Estado miembro de afiliación y del Estado miembro de tratamiento.

2. Cuando difiera el Estado miembro de afiliación de la persona física en tratamiento y el Estado miembro de tratamiento de dicha persona física, el acceso transfronterizo a los datos de salud electrónicos personales de la persona física en tratamiento se proporcionará a través de la infraestructura transfronteriza a que se refiere el artículo 23.

3. El acceso mencionado en los apartados 1 y 2 del presente artículo incluirá, como mínimo, las categorías prioritarias de datos de salud electrónicos personales a que se refiere el artículo 14.

En consonancia con los principios previstos en el artículo 5 del Reglamento (UE) 2016/679, los Estados miembros establecerán reglas relativas a las categorías de datos de salud electrónicos personales accesibles por las diferentes categorías de profesionales sanitarios o a las diferentes tareas de asistencia sanitaria. Dichas reglas tendrán en cuenta la posibilidad de imponer limitaciones en virtud del artículo 8 del presente Reglamento.

4. En caso de tratamiento sanitario en un Estado miembro distinto del Estado miembro de afiliación, las reglas a que se refiere el apartado 3 serán las del Estado miembro de tratamiento.

5. Cuando la persona física haya limitado el acceso a los datos de salud electrónicos personales de conformidad con el artículo 8, no se informará al prestador de asistencia sanitaria ni a los profesionales sanitarios del contenido limitado de dichos datos.

Como excepción a lo dispuesto en el artículo 8, párrafo primero, cuando sea necesario para proteger los intereses vitales del interesado, el prestador de asistencia sanitaria o el profesional sanitario podrán obtener acceso a los datos de salud electrónicos limitados. Dichos casos se registrarán en un formato claro y comprensible y serán fácilmente accesibles para el interesado.

Los Estados miembros podrán incluir garantías adicionales.

Artículo 12

Servicios de acceso para los profesionales sanitarios

En cuanto a la prestación de asistencia sanitaria, los Estados miembros garantizarán que los profesionales sanitarios puedan tener acceso gratuito a las categorías prioritarias de datos de salud electrónicos personales a que se refiere el artículo 14, también en lo referente a la asistencia transfronteriza, a través de los servicios de acceso para los profesionales sanitarios.

Los servicios a que se refiere el párrafo primero del presente artículo solo serán accesibles para los profesionales sanitarios que estén en posesión de medios de identificación electrónica que sean reconocidos con arreglo al artículo 6 del Reglamento (UE) n.º 910/2014 u otros medios de identificación electrónica que cumplan las especificaciones comunes a que se refiere el artículo 36 del presente Reglamento.

Los datos de salud electrónicos personales se presentarán en las historias clínicas electrónicas de manera que los profesionales sanitarios puedan usarlos fácilmente.

Artículo 13

Registro de datos de salud electrónicos personales

1. Los Estados miembros garantizarán que, cuando se traten datos de salud electrónicos para la prestación de asistencia sanitaria, los prestadores de asistencia sanitaria registren los datos de salud electrónicos personales pertinentes pertenecientes, total o parcialmente, al menos a las categorías prioritarias de datos de salud electrónicos personales a que se refiere el artículo 14 en formato electrónico en un sistema HCE.

2. Cuando los prestadores de asistencia sanitaria traten los datos en formato electrónico, garantizarán que los datos de salud electrónicos personales de las personas físicas a las que estén tratando se actualicen con la información relativa a la asistencia sanitaria.

3. Cuando los datos de salud electrónicos personales de una persona física se registren en un Estado miembro de tratamiento distinto del Estado miembro de afiliación de la persona física en cuestión, el Estado miembro de tratamiento garantizará que el registro se realice con los datos de identificación de la persona física en el Estado miembro de afiliación.

4. A más tardar el 26 de marzo de 2027, la Comisión determinará, mediante actos de ejecución, los requisitos para la calidad de los datos, incluidos los relativos a la semántica, la uniformidad, la coherencia, la exactitud y la exhaustividad, para el registro de datos de salud electrónicos personales en un sistema HCE, según proceda. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Cuando se registren o actualicen datos de salud electrónicos personales, en las historias clínicas electrónicas se indicará el profesional sanitario y el prestador de asistencia sanitaria que han realizado dicho registro o actualización, así como el momento en que dicho registro o actualización se han realizado. Los Estados miembros podrán exigir que queden registrados otros aspectos del registro de datos.

Artículo 14

Categorías prioritarias de datos de salud electrónicos personales para uso primario

1. A efectos del presente capítulo, cuando los datos se traten en formato electrónico, las categorías prioritarias de datos de salud electrónicos personales serán las siguientes:

a) las historias clínicas resumidas de los pacientes;

b) las recetas electrónicas;

c) las dispensaciones electrónicas;

d) los estudios de diagnóstico por imagen y los informes de imágenes correspondientes;

e) los resultados de pruebas diagnósticas, incluidos los resultados de laboratorio y otros resultados de diagnóstico e informes correspondientes, y

f) los informes de altas hospitalarias.

Las principales características de las categorías prioritarias de datos de salud electrónicos personales para uso primario serán las que figuran en el anexo I.

Los Estados miembros podrán disponer en su Derecho nacional categorías adicionales de datos de salud electrónicos personales a las que se deba acceder e intercambiar para uso primario con arreglo al presente capítulo.

La Comisión podrá establecer, mediante actos de ejecución, especificaciones transfronterizas para las categorías de datos de salud electrónicos personales a que se refiere el párrafo tercero del presente apartado de conformidad con el artículo 15, apartado 3, y el artículo 23, apartado 8. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 97 para modificar el presente Reglamento por los que se hagan cambios en el anexo I mediante la adición, modificación o supresión de las principales características de las categorías prioritarias de datos de salud electrónicos personales a que se refiere el apartado 1, siempre que la finalidad de los cambios sea adaptar las categorías prioritarias de datos de salud electrónicos personales al progreso técnico y a las normas internacionales. Además, las nuevas características o las modificaciones de aquellas características deberán cumplir los dos criterios siguientes:

a) la característica es pertinente para la asistencia sanitaria prestada a personas físicas;

b) la característica se utiliza en la mayoría de los Estados miembros según la información más reciente.

Artículo 15

Formato europeo de intercambio de historias clínicas electrónicas

1. A más tardar el 26 de marzo de 2027, la Comisión determinará, mediante actos de ejecución, las especificaciones técnicas para las categorías prioritarias de datos de salud electrónicos personales a que se refiere el artículo 14, apartado 1, estableciendo el formato europeo de intercambio de historias clínicas electrónicas. Dicho formato será de uso común, legible por máquina y permitirá la transmisión de datos de salud electrónicos personales entre diferentes aplicaciones informáticas, dispositivos y prestadores de asistencia sanitaria. Dicho formato será compatible con la transmisión de datos de salud estructurados y no estructurados e incluirá los elementos siguientes:

a) conjuntos armonizados de datos que contengan datos de salud electrónicos y definan estructuras, como campos de datos y grupos de datos para la representación del contenido clínico y otras partes de los datos de salud electrónicos;

b) sistemas de codificación y valores que deben utilizarse en los conjuntos de datos que contengan datos de salud electrónicos;

c) especificaciones técnicas de interoperabilidad para el intercambio de datos de salud electrónicos, incluida su representación de contenidos, normas y perfiles.

Los actos de ejecución a que se refiere el párrafo primero del presente apartado se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. La Comisión proporcionará, mediante actos de ejecución, actualizaciones periódicas sobre el formato europeo de intercambio de historias clínicas electrónicas para integrar las revisiones pertinentes de los sistemas y las nomenclaturas de codificación de la asistencia sanitaria. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

3. La Comisión podrá establecer, mediante actos de ejecución, especificaciones técnicas para ampliar el formato europeo de intercambio de historias clínicas electrónicas a categorías adicionales de datos de salud electrónicos personales a que se refiere el artículo 14, apartado 1, párrafo tercero. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

4. Los Estados miembros garantizarán que las categorías prioritarias de datos de salud electrónicos personales a que se refiere el artículo 14 se proporcionen en el formato europeo de intercambio de historias clínicas electrónicas a que se refiere el apartado 1 del presente artículo. Cuando dichos datos se transmitan por medios automatizados para uso primario, el prestador que los reciba aceptará el formato de los datos y los podrá leer.

Artículo 16

Gestión de la identificación

1. Cuando una persona física utilice servicios de acceso a los datos de salud electrónicos a que se refiere el artículo 4, tendrá derecho a identificarse electrónicamente utilizando cualquier medio de identificación electrónica reconocido de conformidad con el artículo 6 del Reglamento (UE) n.º 910/2014. En situaciones transfronterizas, los Estados miembros podrán establecer mecanismos complementarios para garantizar la correspondencia adecuada de las identidades.

2. La Comisión determinará, mediante actos de ejecución, los requisitos para el mecanismo interoperable y transfronterizo de identificación y autenticación para las personas físicas y los profesionales sanitarios, de conformidad con el Reglamento (UE) n.º 910/2014. Dicho mecanismo facilitará la transferibilidad de los datos de salud electrónicos personales en un contexto transfronterizo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

3. La Comisión, en cooperación con los Estados miembros, implementará los servicios requeridos por el mecanismo interoperable y transfronterizo de identificación y autenticación a que se refiere el apartado 2 del presente artículo a escala de la Unión, como parte de la infraestructura transfronteriza a que se refiere el artículo 23.

4. Las autoridades competentes de los Estados miembros y la Comisión implementarán el mecanismo interoperable y transfronterizo de identificación y autenticación a nivel de los Estados miembros y de la Unión, respectivamente.

Artículo 17

Requisitos para la ejecución técnica

La Comisión determinará, mediante actos de ejecución, los requisitos para la ejecución técnica de los derechos establecidos en la presente sección.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 18

Compensación por la puesta a disposición de datos de salud electrónicos personales

Los prestadores que reciban datos en virtud del presente capítulo no estarán obligados a compensar al prestador de asistencia sanitaria por la puesta a disposición de datos de salud electrónicos personales. Los prestadores de asistencia sanitaria o terceros no cobrarán directa ni indirectamente a los interesados tasas ni gastos, ni exigirán compensación alguna por compartir datos o acceder a ellos.

SECCIÓN 2

Gobernanza para el uso primario

Artículo 19

Autoridades de salud digital

1. Cada Estado miembro designará una o varias autoridades de salud digital responsables de la aplicación y el cumplimiento del presente capítulo a escala nacional. El Estado miembro informará a la Comisión sobre la identidad de las autoridades de salud digital a más tardar el 26 de marzo de 2027. Cuando un Estado miembro designe más de una autoridad de salud digital o cuando la autoridad de salud digital esté formada por varias organizaciones, el Estado miembro en cuestión comunicará a la Comisión una descripción del reparto de funciones entre esas diversas autoridades u organizaciones. Cuando un Estado miembro designe varias autoridades de salud digital, designará a una de ellas para que actúe como coordinadora. La Comisión hará pública esa información.

2. Se encomendarán a cada autoridad de salud digital las funciones y competencias siguientes:

a) garantizar la aplicación de los derechos y obligaciones establecidos en el presente capítulo y en el capítulo III mediante la adopción de las soluciones técnicas nacionales, regionales o locales necesarias y el establecimiento de las reglas y mecanismos pertinentes;

b) garantizar que las personas físicas, los profesionales sanitarios y los prestadores de asistencia sanitaria dispongan de información completa y actualizada sobre la aplicación de los derechos y obligaciones establecidos en el presente capítulo y en el capítulo III;

c) para la aplicación de las soluciones técnicas a que se refiere la letra a) del presente apartado, asegurar que dichas soluciones técnicas cumplen con lo dispuesto en el presente capítulo, el capítulo III y el anexo II;

d) contribuir, a escala de la Unión, al desarrollo de soluciones técnicas que permitan a las personas físicas y a los profesionales sanitarios ejercer los derechos y cumplir las obligaciones que les incumben con arreglo al presente capítulo;

e) facilitar a las personas con discapacidad el ejercicio de sus derechos en el marco del presente capítulo, de conformidad con la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo ([31]);

f) supervisar los puntos de contacto nacionales para la salud digital y cooperar con otras autoridades de salud digital y la Comisión en el desarrollo de MiSalud@UE;

g) garantizar la aplicación, a escala nacional, del formato europeo de intercambio de historias clínicas electrónicas, en cooperación con las autoridades nacionales y las partes interesadas;

h) contribuir a escala de la Unión al desarrollo del formato europeo de intercambio de historias clínicas electrónicas, a la elaboración de especificaciones comunes, de conformidad con el artículo 36, relativas a la calidad, la interoperabilidad, la protección, la seguridad, la facilidad de uso, la accesibilidad, la no discriminación o los derechos fundamentales, y a la elaboración de las especificaciones de la base de datos de la UE para sistemas HCE y aplicaciones de bienestar a que se refiere el artículo 49;

i) cuando proceda, realizar actividades de vigilancia del mercado de conformidad con el artículo 43, garantizando al mismo tiempo que se evite cualquier conflicto de intereses;

j) desarrollar la capacidad nacional para aplicar requisitos relativos a la interoperabilidad y la seguridad de datos de salud electrónicos para uso primario y participar en intercambios de información y actividades de desarrollo de capacidades a escala de la Unión;

k) cooperar con las autoridades de vigilancia del mercado, participar en las actividades relacionadas con la gestión de los riesgos que entrañan los sistemas HCE y de los incidentes graves y supervisar la aplicación de medidas correctivas de conformidad con el artículo 44;

l) cooperar con otras entidades y organismos pertinentes a escala local, regional, nacional o de la Unión para garantizar la interoperabilidad, la portabilidad y la seguridad de los datos de salud electrónicos;

([31]) Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios (DO L 151 de 7.6.2019, p. 70).

m) cooperar con las autoridades de control de conformidad con los Reglamentos (UE) n.º 910/2014 y (UE) 2016/679, y la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([32]) y con otras autoridades pertinentes, incluidas las competentes en materia de ciberseguridad e identificación electrónica.

3. Los Estados miembros garantizarán que cada autoridad de salud digital disponga de los recursos humanos, técnicos y financieros, así como de los locales e infraestructuras necesarios para el desempeño efectivo de sus funciones y el ejercicio de sus competencias.

4. En el desempeño de sus funciones, cada autoridad de salud digital evitará todo conflicto de intereses. Cada miembro del personal de la autoridad de salud digital actuará en interés público y de manera independiente.

5. En el desempeño de sus funciones, las autoridades de salud digital pertinentes cooperarán y consultarán activamente con los representantes de las partes interesadas pertinentes, incluidos los representantes de los pacientes, de los prestadores de asistencia sanitaria y de los profesionales sanitarios, incluidas las asociaciones de profesionales sanitarios, así como las organizaciones de consumidores y las asociaciones del sector empresarial.

Artículo 20

Presentación de informes por las autoridades de salud digital

Las autoridades de salud digital designadas de conformidad con el artículo 19 publicarán un informe bienal de actividad que contenga una síntesis general de sus actividades. Si un Estado miembro designa más de una autoridad de salud digital, una de ellas será responsable de la elaboración del informe y, para ello, solicitará la información necesaria a las demás autoridades de salud digital. El informe de actividad seguirá una estructura acordada a nivel de la Unión en el seno del Consejo del Espacio Europeo de Datos de Salud (en lo sucesivo, «Consejo del EEDS») a que se refiere el artículo 92. El informe de actividad contendrá, como mínimo, información sobre:

a) las medidas adoptadas para la aplicación del presente Reglamento;

b) el porcentaje de personas físicas que tiene acceso a las diversas categorías de datos de sus historias clínicas electrónicas;

c) la tramitación de las peticiones de personas físicas relativas al ejercicio de sus derechos en virtud del presente Reglamento;

d) el número de prestadores de asistencia sanitaria de diferentes tipos, incluidas farmacias, hospitales y otros puntos de asistencia que estén conectados a MiSalud@UE, calculado:

   i) en términos absolutos,

   ii) como porcentaje de todos los prestadores de asistencia sanitaria del mismo tipo, y

   iii) como porcentaje de las personas físicas que pueden utilizar los servicios;

e) el volumen de datos de salud electrónicos de diferentes categorías compartidos a través de las fronteras mediante MiSalud@UE;

f) el número de casos de incumplimiento de requisitos obligatorios.

Artículo 21

Derecho a presentar una reclamación ante una autoridad de salud digital

1. Sin perjuicio de cualquier otro recurso administrativo o judicial, las personas físicas y jurídicas tendrán derecho a presentar una reclamación en relación con las disposiciones del presente capítulo, de forma individual o, en su caso, colectiva, ante la autoridad de salud digital competente, siempre que sus derechos o intereses se vean afectados negativamente.

2. Cuando la reclamación se refiera a los derechos de las personas físicas en virtud de los artículos 3 y 5 a 10 del presente Reglamento, la autoridad de salud digital transmitirá la reclamación a las autoridades de control competentes de conformidad con el Reglamento (UE) 2016/679. La autoridad de salud digital proporcionará a la autoridad de control competente de conformidad con el Reglamento (UE) 2016/679 la información necesaria a su disposición a fin de facilitar la evaluación e investigación de la reclamación.

([32]) Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80).

3. La autoridad de salud digital competente ante la que se haya presentado la reclamación informará, de conformidad con el Derecho nacional, al reclamante sobre el estado en que se encuentre la tramitación de la reclamación, sobre la decisión que se tome acerca de la reclamación, sobre toda remisión de la reclamación a la autoridad de control competente en virtud del Reglamento (UE) 2016/679 y, de producirse tal remisión, de que dicha autoridad de control es, desde ese momento, el único punto de contacto para el reclamante en relación con el asunto.

4. Las autoridades de salud digital de los Estados miembros de que se trate cooperarán para tramitar y resolver sin demora indebida las reclamaciones relacionadas con el intercambio transfronterizo y el acceso a datos de salud electrónicos personales, lo que incluirá el intercambio de toda información pertinente por medios electrónicos.

5. Las autoridades de salud digital facilitarán la presentación de reclamaciones y proporcionarán herramientas de fácil acceso para la presentación de las reclamaciones.

Artículo 22

Relación con las autoridades de control del Reglamento (UE) 2016/679

La autoridad o autoridades de control responsables de supervisar y garantizar la aplicación del Reglamento (UE) 2016/679 también serán competentes para supervisar y garantizar la aplicación de los artículos 3 y 5 a 10 del presente Reglamento. Se aplicarán *mutatis mutandis* las disposiciones pertinentes del Reglamento (UE) 2016/679. Las autoridades de control estarán facultadas para imponer multas administrativas hasta el importe mencionado en el artículo 83, apartado 5, del Reglamento (UE) 2016/679.

Las autoridades de control a que se refiere el párrafo primero del presente artículo y las autoridades de salud digital a que se refiere el artículo 19 cooperarán, cuando proceda, en la aplicación del presente Reglamento, en el marco de sus competencias respectivas.

SECCIÓN 3

Infraestructura transfronteriza para el uso primario de datos de salud electrónicos personales

Artículo 23

MiSalud@UE

1. La Comisión establecerá una plataforma central de interoperabilidad para la salud digital («MiSalud@UE») para prestar servicios que apoyen y faciliten el intercambio de datos de salud electrónicos personales entre los puntos de contacto nacionales para la salud digital de los Estados miembros.

2. Cada Estado miembro designará un punto de contacto nacional para la salud digital, como pasarela organizativa y técnica para la prestación de servicios relacionados con el intercambio transfronterizo de datos de salud electrónicos personales en el contexto del uso primario. Cada punto de contacto nacional para la salud digital estará conectado a todos los demás puntos de contacto nacionales para la salud digital en otros Estados miembros y a la plataforma central de interoperabilidad para la salud digital en la infraestructura transfronteriza MiSalud@UE. Cuando un punto de contacto nacional para la salud digital sea una entidad integrada por varias organizaciones responsables de la ejecución de diferentes servicios, el Estado miembro de que se trate comunicará a la Comisión una descripción del reparto de funciones entre las organizaciones. Cada Estado miembro informará a la Comisión sobre la identidad de su punto de contacto nacional para la salud digital a más tardar el 26 de marzo de 2027. El punto de contacto nacional para la salud digital podrá ser designado en el seno de la autoridad de salud digital a que se refiere el artículo 19. Los Estados miembros informarán a la Comisión sobre toda modificación posterior de la identidad de esos puntos de contacto nacionales para la salud digital. La Comisión y los Estados miembros pondrán dicha información a disposición del público.

3. Cada punto de contacto nacional para la salud digital facilitará el intercambio de los datos de salud electrónicos personales a que se refiere el artículo 14, apartado 1, con los puntos de contacto nacionales para la salud digital en otros Estados miembros a través de MiSalud@UE. Dicho intercambio se realizará en el formato europeo de intercambio de historias clínicas electrónicas.

Cuando los Estados miembros establezcan categorías adicionales de datos de salud electrónicos personales en virtud del artículo 14, apartado 1, párrafo tercero, el punto de contacto nacional para la salud digital permitirá el intercambio de las categorías adicionales de datos de salud electrónicos personales a que se refiere el artículo 14, apartado 1, párrafo tercero, en la medida en que el Estado miembro de que se trate haya previsto el acceso a esas categorías adicionales de datos de salud electrónicos personales y su intercambio, de conformidad con el artículo 14, apartado 1, párrafo tercero.

4. A más tardar el 26 de marzo de 2027, la Comisión adoptará, mediante actos de ejecución, las medidas necesarias para el desarrollo técnico de MiSalud@UE, disposiciones pormenorizadas relativas a la seguridad, la confidencialidad y la protección de los datos de salud electrónicos personales, así como las condiciones para las comprobaciones del cumplimiento necesarias para unirse y permanecer conectado a MiSalud@UE. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

5. Los Estados miembros garantizarán la conexión de todos los prestadores de asistencia sanitaria a sus puntos de contacto nacionales para la salud digital. Los Estados miembros garantizarán que los prestadores de asistencia sanitaria conectados puedan realizar intercambios bidireccionales de datos de salud electrónicos con el punto de contacto nacional para la salud digital.

6. Los Estados miembros garantizarán que las farmacias que operen en sus territorios, incluidas las farmacias en línea, puedan dispensar recetas electrónicas expedidas en otros Estados miembros, en las condiciones establecidas en el artículo 11 de la Directiva 2011/24/UE.

Las farmacias accederán a las recetas electrónicas que se les transmitan desde otros Estados miembros a través de MiSalud@UE, y deberán aceptarlas, siempre que se cumplan las condiciones establecidas en el artículo 11 de la Directiva 2011/24/UE.

Tras la dispensación de medicamentos a partir de una receta electrónica de otro Estado miembro, la farmacia de que se trate notificará a través de MiSalud@UE dicha dispensación al punto de contacto nacional para la salud digital del Estado miembro en el que se haya expedido dicha receta.

7. Los puntos de contacto nacionales para la salud digital actuarán como corresponsables del tratamiento de los datos de salud electrónicos personales comunicados a través de MiSalud@UE para las operaciones de tratamiento en las que participen. La Comisión actuará como encargada del tratamiento.

8. La Comisión establecerá, mediante actos de ejecución, disposiciones relativas a los requisitos de ciberseguridad, interoperabilidad técnica, interoperabilidad semántica, operaciones y gestión de servicios en relación con el tratamiento por parte del encargado del tratamiento a que se refiere el apartado 7 del presente artículo y sus responsabilidades con respecto a los responsables del tratamiento, de conformidad con el capítulo IV del Reglamento (UE) 2016/679. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

9. Los puntos de contacto nacionales para la salud digital cumplirán las condiciones para unirse y permanecer conectados a MiSalud@UE, tal como se establece en los actos de ejecución a que se refiere el apartado 4. La Comisión verificará el cumplimiento por parte de los puntos de contacto nacionales para la salud digital mediante comprobaciones del cumplimiento.

Artículo 24

Servicios e infraestructuras de salud digital transfronterizos complementarios

1. Los Estados miembros podrán prestar a través de MiSalud@UE servicios complementarios que faciliten la telemedicina, la salud móvil, el acceso de las personas físicas a toda traducción existente de sus datos de salud, el intercambio o la verificación de certificados relacionados con la salud, incluidos los servicios de carnés de vacunación que apoyan la salud pública y su seguimiento o los sistemas, los servicios y las aplicaciones interoperables de salud digital, con vistas a lograr un elevado nivel de confianza y seguridad, mejorar la continuidad de la asistencia y garantizar el acceso a una asistencia sanitaria segura y de calidad. La Comisión establecerá, mediante actos de ejecución, los aspectos técnicos de esos servicios complementarios. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. La Comisión y los Estados miembros podrán facilitar el intercambio de datos de salud electrónicos personales con otras infraestructuras, como el Sistema de Gestión Clínica de Pacientes u otros servicios o infraestructuras en los ámbitos de la salud, la asistencia o la seguridad social que puedan convertirse en participantes autorizados en MiSalud@UE. La Comisión establecerá, mediante actos de ejecución, los aspectos técnicos de esos intercambios. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

La conexión de otra infraestructura a la plataforma central para la salud digital, y su desconexión de esta, necesitarán de una decisión de la Comisión adoptada mediante un acto de ejecución, basada en el resultado de las comprobaciones del cumplimiento de conformidad de los aspectos técnicos de los intercambios a que se refiere el párrafo primero del presente apartado. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

3. Un punto de contacto nacional para la salud digital de un tercer país o un sistema establecido a nivel internacional por una organización internacional podrá convertirse en un participante autorizado en MiSalud@UE siempre que cumpla los requisitos de MiSalud@UE a efectos del intercambio de datos de salud electrónicos personales a que se refiere el artículo 23, que la transferencia derivada de la conexión a MiSalud@UE cumpla lo dispuesto en el capítulo V del Reglamento (UE) 2016/679 y que los requisitos relativos a las medidas jurídicas, organizativas, operativas, semánticas, técnicas y de ciberseguridad sean equivalentes a los aplicables a los Estados miembros en la gestión de los servicios de MiSalud@UE. La Comisión verificará dichos requisitos mediante comprobaciones del cumplimiento.

Sobre la base de los resultados de las comprobaciones del cumplimiento a que se refiere el párrafo primero del presente apartado, la Comisión podrá decidir, mediante actos de ejecución, conectar al punto de contacto nacional para la salud digital del tercer país o el sistema establecido a nivel internacional por una organización internacional, a MiSalud@UE o desconectarlo de esta, según el caso. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

La Comisión establecerá y mantendrá una lista de puntos de contacto nacionales para la salud digital de terceros países o de sistemas establecidos a nivel internacional por organizaciones internacionales conectados a MiSalud@UE de conformidad con el presente apartado y pondrá dicha lista a disposición del público.

CAPÍTULO III

SISTEMAS HCE Y APLICACIONES DE BIENESTAR

SECCIÓN 1

Ámbito de aplicación y disposiciones generales en lo que respecta a los sistemas HCE

Artículo 25

Componentes armonizados de programa informático de sistemas HCE

1. Los sistemas HCE incluirán un componente de programa informático europeo de interoperabilidad para sistemas HCE y un componente de programa informático europeo de registro para sistemas HCE (en lo sucesivo, «componentes armonizados de programa informático de sistemas HCE»), de conformidad con las disposiciones establecidas en el presente capítulo.

2. El presente capítulo no se aplicará a los programas informáticos de propósito general utilizados en un entorno de asistencia sanitaria.

Artículo 26

Introducción en el mercado y puesta en servicio

1. Los sistemas HCE solo podrán introducirse en el mercado o ponerse en servicio si cumplen lo dispuesto en el presente capítulo.

2. Se considerarán puestos en servicio los sistemas HCE que se fabriquen y utilicen en centros sanitarios establecidos en la Unión, así como los sistemas HCE que se ofrezcan como un servicio tal como se define en el artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo ([33]) a una persona física o jurídica establecida en la Unión.

3. Los Estados miembros no podrán prohibir o restringir la introducción en el mercado de sistemas HCE que cumplan lo dispuesto en el presente Reglamento, por consideraciones referidas a aspectos relacionados con los componentes armonizados de programa informático de los sistemas HCE regulados por el presente Reglamento.

Artículo 27

Relación con el Derecho de la Unión que regula los productos sanitarios, los productos sanitarios para diagnóstico* in vitro *y los sistemas de IA

1. Los fabricantes de productos sanitarios o de productos sanitarios para diagnóstico *in vitro*, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) 2017/745 y el artículo 2, punto 2, del Reglamento (UE) 2017/746, respectivamente, que declaren la interoperabilidad de dichos productos sanitarios o productos sanitarios para diagnóstico en vitro con los componentes armonizados de programa informático de los sistemas HCE deberán demostrar la

([33]) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

conformidad con los requisitos esenciales aplicables al componente de programa informático europeo de interoperabilidad para sistemas HCE y al componente de programa informático europeo de registro para sistemas HCE establecidos en el anexo II, sección 2, del presente Reglamento. El artículo 36 del presente Reglamento será aplicable a dichos productos sanitarios y productos sanitarios para diagnóstico *in vitro*.

2. Los proveedores de sistemas de IA considerados de alto riesgo de conformidad con el artículo 6 del Reglamento (UE) 2024/1689 (en lo sucesivo, «sistemas de IA de alto riesgo») y que no están incluidos en el ámbito de aplicación de los Reglamentos (UE) 2017/745 o (UE) 2017/746, que declaren la interoperabilidad de dichos sistemas de IA de alto riesgo con los componentes armonizados de programa informático de los sistemas HCE, deberán demostrar que cumplen los requisitos esenciales aplicables al componente de programa informático europeo de interoperabilidad para sistemas HCE y al componente de programa informático europeo de registro para sistemas HCE establecidos en el anexo II, sección 2, del presente Reglamento. El artículo 36 del presente Reglamento será aplicable a dichos sistemas de IA de alto riesgo.

Artículo 28

Declaraciones

Queda prohibido utilizar en la ficha informativa, en las instrucciones de uso o en cualquier otra información que acompañe a los sistemas HCE, y en la publicidad de estos sistemas, textos, denominaciones, marcas comerciales, fotografías e imágenes u otros signos que puedan inducir a error a los usuarios profesionales tal como se definen en el artículo 3, punto 8, del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo ([34]) en cuanto a la finalidad prevista, la interoperabilidad y la seguridad de los sistemas por alguno de los siguientes medios:

a) atribuir al sistema HCE funciones y propiedades que no posee;

b) no informar al usuario profesional de las posibles limitaciones relacionadas con la interoperabilidad o las características de seguridad del sistema HCE en relación con su finalidad prevista;

c) sugerir usos del sistema HCE distintos de los que se indica que forman parte de la finalidad prevista en la documentación técnica.

Artículo 29

Adquisición, reembolso y financiación

Los Estados miembros podrán mantener o elaborar reglas específicas para la adquisición, el reembolso o la financiación de los sistemas HCE en el contexto de la organización, prestación o financiación de servicios de asistencia sanitaria, siempre que tales reglas cumplan el Derecho de la Unión y no afecten al funcionamiento de los componentes armonizados de programa informático de los sistemas HCE o a su conformidad.

SECCIÓN 2

Obligaciones de los operadores económicos con respecto a los sistemas HCE

Artículo 30

Obligaciones de los fabricantes de sistemas HCE

1. Los fabricantes de sistemas HCE:

a) garantizarán que los componentes armonizados de programa informático de sus sistemas HCE y los propios sistemas HCE, en la medida en que en el presente capítulo se establezcan requisitos al respecto, sean conformes con los requisitos esenciales establecidos en el anexo II y con las especificaciones comunes de conformidad con el artículo 36;

b) garantizarán que los componentes armonizados de programa informático de sus sistemas HCE no se vean afectados negativamente por otros componentes de programa informático del mismo sistema HCE;

c) elaborarán la documentación técnica de sus sistemas HCE de conformidad con el artículo 37 antes de introducir en el mercado dichos sistemas HCE, y posteriormente la mantendrán actualizada;

([34]) Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (DO L 303 de 28.11.2018, p. 59).

d) garantizarán que sus sistemas HCE vayan acompañados, de forma gratuita para el usuario, de la ficha informativa prevista en el artículo 38 y de instrucciones de uso claras y completas;

e) elaborarán la declaración UE de conformidad con arreglo al artículo 39;

f) colocarán el marcado CE de conformidad con arreglo al artículo 41;

g) indicarán en el sistema HCE el nombre, el nombre comercial registrado o marca comercial registrada, la dirección postal y el sitio web, la dirección de correo electrónico o cualquier otro dato de contacto digital mediante el que se les pueda contactar; indicarán en los datos de contacto un punto de contacto único en el que se pueda contactar al fabricante; los datos de contacto se redactarán en una lengua que sea fácil de comprender por los usuarios y autoridades de vigilancia del mercado;

h) cumplirán las obligaciones de registro a que se refiere el artículo 49;

i) adoptarán sin demora indebida las medidas correctivas que resulten necesarias en relación con sus HCE cuando estimen o tengan motivos para creer que dichos sistemas no son conformes con los requisitos esenciales establecidos en el anexo II o han dejado de serlo, o recuperarán o retirarán esos sistemas; a continuación, los fabricantes de sistemas HCE informarán a las autoridades nacionales de los Estados miembros en los que hayan comercializado o puesto en servicio sus sistemas HCE acerca de la no conformidad, de las medidas correctivas adoptadas, incluido el calendario de aplicación, y de la fecha de puesta en conformidad o de recuperación o retirada de los componentes armonizados de programa informático de sus sistemas HCE;

j) informarán a los distribuidores de sus sistemas HCE y, en su caso, al representante autorizado, a los importadores y a los usuarios de la no conformidad y de toda medida correctiva o de la recuperación o retirada de dichos sistemas HCE;

k) informarán a los distribuidores de sus sistemas HCE —y, en su caso, al representante autorizado, a los importadores y a los usuarios— de cualquier mantenimiento preventivo obligatorio de los sistemas HCE y de la frecuencia de este;

l) proporcionarán, a petición de un Estado miembro y en una lengua oficial de este, a las autoridades de vigilancia del mercado de dicho Estado miembro toda la información y documentación necesarias para demostrar la conformidad de los sistemas HCE que hayan introducido en el mercado o puesto en servicio con los requisitos esenciales establecidos en el anexo II;

m) cooperarán con las autoridades de vigilancia del mercado, a petición de estas, en cualquier medida destinada a adaptar los sistemas HCE que hayan introducido en el mercado o puesto en servicio a los requisitos esenciales establecidos en el anexo II y a cualquier requisito adoptado en virtud del artículo 42, en una lengua oficial del Estado miembro de que se trate;

n) establecerán canales de reclamación y mantendrán informados de ello a los distribuidores;

o) llevarán un registro de las reclamaciones y un registro de los sistemas HCE no conformes, y mantendrán informados de ello a los distribuidores.

2. Los fabricantes de sistemas HCE se asegurarán de que existen procedimientos para garantizar que el diseño, el desarrollo y la implantación de los componentes armonizados de programa informático de un sistema HCE siguen cumpliendo los requisitos esenciales establecidos en el anexo II y las especificaciones comunes a que se refiere el artículo 36. Los cambios en el diseño o las características del sistema HCE en relación con los componentes armonizados de programa informático se tendrán debidamente en cuenta y se reflejarán en la documentación técnica.

3. Los fabricantes de sistemas HCE conservarán la documentación técnica a que se refiere el artículo 37 y la declaración UE de conformidad a que se refiere el artículo 39 durante diez años a partir de la introducción en el mercado del sistema HCE cubierto por la declaración UE de conformidad.

Los fabricantes de sistemas HCE pondrán a disposición de las autoridades pertinentes, previa solicitud motivada, el código fuente o la lógica de programación que se incluya en la documentación técnica, si ese código fuente o esa lógica de programación fuesen necesarios para que dichas autoridades puedan comprobar el cumplimiento de los requisitos esenciales establecidos en el anexo II.

4. Cualquier fabricante de sistemas HCE establecido fuera de la Unión garantizará que su representante autorizado dispone de la documentación necesaria para cumplir las funciones a que se refiere el artículo 31, apartado 2.

5. Previa solicitud motivada de una autoridad de vigilancia del mercado, los fabricantes de sistemas HCE le proporcionarán toda la información y documentación necesarias para demostrar la conformidad del sistema HCE con los requisitos esenciales establecidos en el anexo II y las especificaciones comunes a que se refiere el artículo 36, bien en papel o bien en formato electrónico y redactadas en una lengua que sea fácil de comprender por dicha autoridad de vigilancia del mercado. Los fabricantes de sistemas HCE cooperarán con la autoridad de vigilancia del mercado, a petición de esta, en cualquier medida que se adopte para eliminar los riesgos que entrañe un sistema HCE que hayan introducido en el mercado o puesto en servicio.

Artículo 31

Representantes autorizados

1. Antes de comercializar un sistema HCE en la Unión, un fabricante de sistemas HCE establecido fuera de la Unión tendrá que designar, mediante mandato escrito, a un representante autorizado que esté establecido en el territorio de la Unión.

2. El representante autorizado efectuará las funciones especificadas en el mandato acordado con el fabricante. El mandato deberá permitir al representante autorizado desempeñar como mínimo las funciones siguientes:

a) mantener la declaración UE de conformidad y la documentación técnica a que se refiere el artículo 37 a disposición de las autoridades de vigilancia del mercado durante el período contemplado en el artículo 30, apartado 3;

b) entregar a las autoridades de los Estados miembros de que se trate, previa solicitud motivada de una autoridad de vigilancia del mercado, una copia del mandato y toda la información y documentación necesarias para demostrar la conformidad del sistema HCE con los requisitos esenciales establecidos en el anexo II y con las especificaciones comunes a que se refiere el artículo 36;

c) informar sin demora indebida al fabricante si el representante autorizado tiene motivos para creer que un sistema HCE ya no es conforme con los requisitos esenciales establecidos en el anexo II;

d) informar sin demora indebida al fabricante de cualquier reclamación recibida de los consumidores o de los usuarios profesionales;

e) cooperar con las autoridades de vigilancia del mercado, a petición de estas, en cualquier medida correctiva adoptada en relación con los sistemas HCE cubiertos por su mandato;

f) poner fin al mandato si el fabricante no cumple las obligaciones que le incumben en virtud del presente Reglamento;

g) asegurar que la documentación técnica a que se refiere el artículo 37 pueda ponerse a disposición de las autoridades pertinentes, cuando así se solicite.

3. En caso de cambio del representante autorizado, las medidas detalladas para dicho cambio abordarán, como mínimo, lo siguiente:

a) la fecha de terminación del mandato del representante autorizado anterior y la de comienzo del mandato del nuevo representante autorizado;

b) la transferencia de documentos, incluidos los aspectos relacionados con la confidencialidad y los derechos de propiedad.

4. Cuando el fabricante esté establecido fuera de la Unión y no haya cumplido las obligaciones formuladas en el artículo 30, el representante autorizado será responsable solidario en caso de incumplimiento del presente Reglamento con arreglo al mismo fundamento que el fabricante.

Artículo 32

Obligaciones de los importadores

1. Los importadores introducirán en el mercado de la Unión únicamente sistemas HCE que sean conformes con los requisitos esenciales establecidos en el anexo II, así como con las especificaciones comunes a que se refiere el artículo 36.

2. Antes de comercializar un sistema HCE, los importadores se asegurarán de que:

a) el fabricante ha elaborado la documentación técnica a que se refiere el artículo 37 y la declaración UE de conformidad;

b) el fabricante está identificado y se ha designado un representante autorizado con arreglo al artículo 31;

c) el sistema HCE lleva el marcado CE de conformidad a que se refiere el artículo 41 una vez concluido el procedimiento de evaluación de la conformidad;

d) el sistema HCE va acompañado de la ficha informativa a que se refiere el artículo 38 con instrucciones de uso claras y completas, que abarquen también su mantenimiento, en formatos accesibles.

3. Los importadores indicarán su nombre, su nombre comercial registrado o marca comercial registrada, su dirección postal, sitio web, dirección de correo electrónico o cualquier otro dato de contacto digital con el que se les pueda contactar, en un documento que acompañe al sistema HCE. Los datos de contacto indicarán un punto de contacto único en el que se pueda contactar al fabricante y se redactarán en una lengua que sea fácil de comprender por los usuarios y las autoridades de vigilancia del mercado. Los importadores garantizarán que la información proporcionada por el fabricante que figure en cualquier etiqueta original proporcionada con el sistema HCE no quede oculta por alguna otra etiqueta adicional.

4. Los importadores se asegurarán de que, mientras esté bajo su responsabilidad, el sistema HCE no se altere de manera que se comprometa su conformidad con los requisitos esenciales establecidos en el anexo II y con cualquier requisito adoptado en virtud del artículo 42.

5. Cuando un importador considere o tenga motivos para creer que un sistema HCE no es conforme con los requisitos esenciales establecidos en el anexo II y con cualquier requisito adoptado en virtud del artículo 42, o ha dejado de serlo, no lo comercializará hasta que se ponga en conformidad o, si dicho sistema HCE ya había sido introducido en el mercado, lo recuperará o retirará hasta su puesta en conformidad. En caso de que se produzca dicha recuperación o retirada, el importador informará de ello sin demora indebida al fabricante del sistema HCE, a los usuarios y a las autoridades de vigilancia del mercado del Estado miembro en el que lo haya comercializado, dando detalles, en particular, de la no conformidad de alguna medida correctiva adoptada.

Cuando un importador estime o tenga motivos para creer que un sistema HCE presenta un riesgo para la salud o la seguridad de las personas físicas, informará de ello sin demora indebida a las autoridades de vigilancia del mercado del Estado miembro en que esté establecido, así como al fabricante y, en su caso, al representante autorizado.

6. Los importadores conservarán una copia de la declaración UE de conformidad a disposición de las autoridades de vigilancia del mercado durante el período a que se refiere el artículo 30, apartado 3, y se asegurarán de que la documentación técnica a que se refiere el artículo 37 pueda ponerse a disposición de dichas autoridades, previa solicitud.

7. Previa solicitud motivada de las autoridades de vigilancia del mercado de los Estados miembros de que se trate, los importadores les proporcionarán la información y documentación necesarias para demostrar la conformidad de un sistema HCE. Los importadores cooperarán con dichas autoridades, a petición de estas, así como con el fabricante y, en su caso, con el representante autorizado, en una lengua oficial del Estado miembro en el que esté establecida la autoridad de vigilancia del mercado. Los importadores cooperarán con dichas autoridades, a petición de estas, en cualquier medida destinada a adaptar sus sistemas HCE a los requisitos esenciales en relación con los componentes armonizados de programa informático tal como se dispone en el anexo II o a garantizar que los sistemas HCE que no sean conformes con dichos requisitos esenciales se recuperen o retiren.

8. Los importadores establecerán canales de denuncia y garantizarán que sean accesibles para que los usuarios puedan presentar reclamaciones, y llevarán un registro de las reclamaciones, de los sistemas HCE no conformes y de las recuperaciones y retiradas de sistemas HCE. Los importadores verificarán que los canales de denuncia establecidos con arreglo al artículo 30, apartado 1, letra n), estén públicamente disponibles y permitan a los usuarios presentar reclamaciones y recibir toda comunicación relativa a cualquier riesgo relacionado con la salud y la seguridad o con otros aspectos de la protección del interés público y permitan a los usuarios estar informados de cualquier incidente grave que afecte a un sistema HCE. Cuando tales canales de denuncia no hayan sido establecidos, los importadores los establecerán y tendrán en cuenta las necesidades en materia de accesibilidad de los grupos vulnerables y las personas con discapacidad.

9. Los importadores investigarán las reclamaciones y realizarán un seguimiento de la información recibida relativa a incidentes que afecten a un sistema HCE que hayan comercializado. Los importadores registrarán dichas reclamaciones, las recuperaciones y retiradas de sistemas HCE, y cualquier medida correctiva adoptada para poner en conformidad el sistema HCE, en el registro a que se refiere el artículo 30, apartado 1, letra o), o en su propio registro interno. Los importadores mantendrán informados de la investigación y el seguimiento realizados y de sus resultados, de manera oportuna, al fabricante, a los distribuidores y, cuando proceda, a los representantes autorizados.

Artículo 33

Obligaciones de los distribuidores

1. Antes de comercializar un sistema HCE, los distribuidores comprobarán que:

a) el fabricante ha elaborado la declaración UE de conformidad;

b) el sistema HCE lleva el marcado CE de conformidad;

c) el sistema HCE va acompañado de la ficha informativa a que se refiere el artículo 38 con instrucciones de uso claras y completas en formatos accesibles;

d) en su caso, el importador ha cumplido los requisitos establecidos en el artículo 32, apartado 3.

2. Los distribuidores se asegurarán de que, mientras esté bajo su responsabilidad, el sistema HCE no se vea alterado de manera que se comprometa su conformidad con los requisitos esenciales establecidos en el anexo II y con cualquier requisito adoptado en virtud del artículo 42.

3. Cuando un distribuidor considere o tenga motivos para creer que un sistema HCE no es conforme con los requisitos esenciales del anexo II y con cualquier requisito adoptado en virtud del artículo 42, no podrá comercializarlo hasta que se haya puesto en conformidad. El distribuidor informará de ello sin demora indebida al fabricante o al importador, así como a las autoridades de vigilancia del mercado de los Estados miembros en los que se haya comercializado el sistema HCE o vaya a ser comercializado. Cuando un distribuidor considere o tenga motivos para creer que un sistema HCE presenta un riesgo para la salud o seguridad de las personas físicas, informará a las autoridades de vigilancia del mercado del Estado miembro en que esté establecido, así como al fabricante y al importador.

4. Previa solicitud motivada de una autoridad de vigilancia del mercado, los distribuidores le proporcionarán la información y documentación necesarias para demostrar la conformidad del sistema HCE. Cooperarán con dicha autoridad, a petición de esta, así como con el fabricante, el importador y, en su caso, el representante autorizado del fabricante, en cualquier medida destinada a adaptar un sistema HCE a los requisitos esenciales establecidos en el anexo II y con cualquier requisito adoptado en virtud del artículo 42, o a recuperarlos o retirarlos.

Artículo 34

Casos en los que las obligaciones de los fabricantes de sistemas HCE se aplican a otras entidades o personas físicas

Se considerarán fabricantes a los efectos del presente Reglamento y tendrán que cumplir las obligaciones establecidas en el artículo 30, los importadores, distribuidores o usuarios que:

a) comercialicen un sistema HCE con su nombre comercial o marca;

b) modifiquen un sistema HCE que ya haya sido introducido en el mercado de tal manera que pueda verse afectada su conformidad con los requisitos aplicables, o

c) modifiquen un sistema HCE de tal manera que genere cambios en la finalidad prevista declarada por el fabricante.

Artículo 35

Identificación de los operadores económicos

Los operadores económicos identificarán, previa solicitud, ante las autoridades de vigilancia del mercado, durante diez años a partir de la fecha de introducción en el mercado del último sistema HCE cubierto por la declaración UE de conformidad:

a) a cualquier operador económico que les haya suministrado un sistema HCE, y

b) a cualquier operador económico al que hayan suministrado un sistema HCE.

SECCIÓN 3

Conformidad de los componentes armonizados de programa informático de sistemas HCE

Artículo 36

Especificaciones comunes

1. A más tardar el 26 de marzo de 2027, la Comisión adoptará, mediante actos de ejecución, especificaciones comunes con respecto a los requisitos esenciales establecidos en el anexo II, que incluirán un modelo común y un plazo para la aplicación de esas especificaciones comunes. Cuando proceda, dichas especificaciones comunes tendrán en cuenta las especificidades de los productos sanitarios y los sistemas de IA de alto riesgo a que se refiere el artículo 27, apartados 1 y 2, respectivamente, incluidas las normas más avanzadas en materia de informática sanitaria y el formato europeo de intercambio de historias clínicas electrónicas. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

2. Entre las especificaciones comunes a que se refiere el apartado 1, se incluirán la información y elementos siguientes:

a) su ámbito de aplicación;

b) su aplicabilidad a las diferentes categorías de sistemas HCE o de las funciones que abarquen;

c) su versión;

d) su período de validez;

e) una parte normativa;

f) una parte explicativa, incluidas las directrices de aplicación pertinentes.

3. Las especificaciones comunes a que se refiere el apartado 1 podrán incluir elementos relacionados con lo siguiente:

a) conjuntos de datos que contengan datos de salud electrónicos y definan estructuras, como campos de datos y grupos de datos para la representación del contenido clínico y otras partes de los datos de salud electrónicos;

b) sistemas de codificación y valores que deben utilizarse en los conjuntos de datos que contengan datos de salud electrónicos, teniendo debidamente en cuenta tanto una posible armonización futura de las terminologías como su compatibilidad con las terminologías nacionales existentes;

c) otros requisitos relacionados con la calidad de los datos, como la exhaustividad y exactitud de los datos de salud electrónicos;

d) especificaciones técnicas, normas y perfiles para el intercambio de datos de salud electrónicos;

e) requisitos y principios relacionados con la seguridad de los pacientes y la seguridad, la confidencialidad, la integridad y la protección de los datos de salud electrónicos;

f) especificaciones y requisitos relacionados con la gestión de la identificación y el uso de la identificación electrónica.

4. Los sistemas HCE, los productos sanitarios, los productos sanitarios para diagnóstico *in vitro* y los sistemas de IA de alto riesgo a que se refieren los artículos 25 y 27 que sean conformes con las especificaciones comunes a que se refiere el apartado 1 del presente artículo, se considerarán conformes con los requisitos esenciales cubiertos por dichas especificaciones comunes o partes de ellas, establecidos en el anexo II, y cubiertos por dichas especificaciones comunes o las correspondientes partes de ellas.

5. Cuando las especificaciones comunes relativas a los requisitos de interoperabilidad y seguridad de los sistemas HCE afecten a productos sanitarios, productos sanitarios para diagnóstico *in vitro* o sistemas de IA de alto riesgo incluidos en el ámbito de aplicación de otros actos jurídicos, como los Reglamentos (UE) 2017/745, (UE) 2017/746 o (UE) 2024/1689, la adopción de esas especificaciones comunes podrá ir precedida de una consulta al Grupo de Coordinación de Productos Sanitarios (MDCG) creado por el artículo 103 del Reglamento (UE) 2017/745 o al Comité Europeo de Inteligencia Artificial creado por el artículo 65 del Reglamento (UE) 2024/1689 y al Comité Europeo de Protección de Datos (CEPD), según proceda.

6. Cuando las especificaciones comunes relativas a los requisitos de interoperabilidad y seguridad de los productos sanitarios, productos sanitarios para diagnóstico *in vitro* o sistemas de IA de alto riesgo incluidos en el ámbito de aplicación de otros actos jurídicos, como los Reglamentos (UE) 2017/745, (UE) 2017/746 o (UE) 2024/1689 afecten a los sistemas HCE, la Comisión garantizará que la adopción de esas especificaciones comunes vaya precedida de una consulta al Consejo del EEDS y al CEPD, según proceda.

Artículo 37

Documentación técnica

1. Los fabricantes elaborarán la documentación técnica antes de la introducción en el mercado o puesta en servicio del sistema HCE, y mantendrán esa documentación actualizada.

2. La documentación técnica a que se refiere el apartado 1 del presente artículo demostrará que el sistema HCE cumple los requisitos esenciales establecidos en el anexo II y proporcionará a las autoridades de vigilancia del mercado toda la información necesaria para evaluar si el sistema HCE es conforme con tales requisitos. Esa documentación técnica contendrá, como mínimo, los elementos contemplados en el anexo III y una referencia a los resultados obtenidos en un entorno digital de pruebas europeo según lo dispuesto en el artículo 40.

3. La documentación técnica a que se refiere el apartado 1 se redactará en una lengua oficial del Estado miembro de que se trate o en una lengua que sea fácil de comprender en dicho Estado miembro. Previa solicitud motivada de la autoridad de vigilancia del mercado de un Estado miembro, el fabricante proporcionará una traducción de las partes pertinentes de la documentación técnica en una lengua oficial de dicho Estado miembro.

4. Cuando una autoridad de vigilancia del mercado solicite al fabricante la documentación técnica o la traducción de partes de esta, el fabricante proporcionará dicha documentación técnica o traducción en un plazo de treinta días a partir de la fecha de la solicitud, salvo que un riesgo grave e inmediato justifique un plazo más corto. Si el fabricante no cumple los requisitos de los apartados 1, 2 y 3 del presente artículo, la autoridad de vigilancia del mercado podrá exigirle que encargue a un organismo independiente, a sus expensas, la realización de una prueba en un plazo determinado con el fin de verificar la conformidad con los requisitos esenciales establecidos en el anexo II y con las especificaciones comunes a que se refiere el artículo 36.

Artículo 38

Ficha informativa que acompaña al sistema HCE

1. Los sistemas HCE irán acompañados de una ficha informativa que incluya información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios profesionales.

2. La ficha informativa a que se refiere el apartado 1 especificará:

a) la identidad, el nombre comercial registrado o la marca registrada, y los datos de contacto del fabricante y, en su caso, de su representante autorizado;

b) el nombre y la versión del sistema HCE y la fecha de su puesta en servicio;

c) la finalidad prevista del sistema HCE;

d) las categorías de datos de salud electrónicos para cuyo tratamiento el sistema HCE ha sido diseñado;

e) las normas, formatos y especificaciones con los que funciona el sistema HCE, y las versiones de dichas normas, formatos y especificaciones.

3. En lugar de suministrar con el sistema HCE la ficha de información a que se refiere el apartado 1 del presente artículo, los fabricantes podrán introducir la información a que se refiere el apartado 2 del presente artículo en la base de datos de la UE para el registro de los sistemas HCE y de las aplicaciones de bienestar a que se refiere el artículo 49.

Artículo 39

Declaración UE de conformidad

1. La declaración UE de conformidad a que se refiere el artículo 30, apartado 1, letra e), indicará que el fabricante de un sistema HCE ha demostrado que se cumplen los requisitos esenciales establecidos en el anexo II.

2. Cuando, en lo que atañe a aspectos que no son objeto del presente Reglamento, un sistema HCE se incluya en el ámbito de aplicación de otros actos jurídicos de la Unión que también requieran por parte del fabricante una declaración UE de conformidad en la que se acredite el cumplimiento de los requisitos de dichos actos jurídicos, se elaborará una única declaración UE de conformidad relativa a todos los actos jurídicos de la Unión aplicables al sistema HCE. Esa declaración UE de conformidad contendrá toda la información necesaria para determinar los actos jurídicos de la Unión a los que se refiere.

3. La declaración UE de conformidad contendrá la información indicada en el anexo IV y se traducirá a la lengua o lenguas oficiales de la Unión que determinen los Estados miembros en que se comercialice el sistema HCE.

4. Cuando la declaración UE de conformidad se elabore en formato digital, será accesible en línea durante la vida útil prevista del sistema HCE y, en cualquier caso, durante al menos los diez años a partir de la introducción en el mercado o la puesta en servicio del sistema HCE.

5. Mediante la elaboración de la declaración UE de conformidad, el fabricante asumirá la responsabilidad de la conformidad de los componentes armonizados de programa informático del sistema HCE con los requisitos establecidos en el presente Reglamento en el momento de su introducción en el mercado o puesta en servicio.

6. La Comisión publicará un modelo normalizado uniforme de declaración UE de conformidad y lo pondrá a disposición en formato digital en todas las lenguas oficiales de la Unión.

Artículo 40

Entorno digital de pruebas europeo

1. La Comisión desarrollará un entorno digital de pruebas europeo para la evaluación de los componentes armonizados de programa informático de los sistemas HCE. La Comisión pondrá a disposición como código abierto el programa informático en el que se base el entorno digital de pruebas europeo.

2. Los Estados miembros explotarán entornos digitales de pruebas para la evaluación de los componentes armonizados de programa informático de los sistemas HCE. Dichos entornos digitales de pruebas cumplirán las especificaciones comunes para el entorno digital de pruebas europeo establecidas de conformidad con el apartado 4. Los Estados miembros informarán a la Comisión acerca de sus entornos digitales de pruebas.

3. Antes de introducir en el mercado un sistema HCE, los fabricantes utilizarán los entornos digitales de pruebas a que se refieren los apartados 1 y 2 del presente artículo para la evaluación de los componentes armonizados de programa informático de los sistemas HCE. Los resultados de dicha evaluación se incluirán en la documentación técnica a que se refiere el artículo 37. Los elementos respecto de los cuales los resultados de la evaluación sean positivos se presumirán conformes al presente Reglamento.

4. La Comisión establecerá, mediante actos de ejecución, las especificaciones comunes para el entorno digital de pruebas europeo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 41

Marcado CE de conformidad

1. El marcado CE de conformidad se colocará de manera visible, legible e indeleble en los documentos que acompañan al sistema HCE y, en su caso, en el embalaje del sistema HCE.

2. El marcado CE de conformidad se colocará antes de introducir en el mercado el sistema HCE.

3. Los principios generales establecidos en el artículo 30 del Reglamento (CE) n.º 765/2008 se aplicarán al marcado CE de conformidad.

Artículo 42

Requisitos nacionales y notificación a la Comisión

1. Los Estados miembros podrán adoptar requisitos nacionales para los sistemas HCE y disposiciones sobre la evaluación de su conformidad en relación con aspectos distintos de los componentes armonizados de programa informático de los sistemas HCE.

2. Los requisitos o las disposiciones nacionales a que se refiere el apartado 1 no deberán afectar negativamente a los componentes armonizados de programa informático de los sistemas HCE.

3. Cuando los Estados miembros adopten requisitos o disposiciones con arreglo al apartado 1, informarán de ello a la Comisión.

SECCIÓN 4

Vigilancia del mercado para los sistemas HCE

Artículo 43

Autoridades de vigilancia del mercado

1. El Reglamento (UE) 2019/1020 se aplicará a los sistemas HCE en relación con los requisitos aplicables a los sistemas regulados en el presente capítulo, y los riesgos que entrañan dichos sistemas.

2. Los Estados miembros designarán la autoridad o las autoridades de vigilancia del mercado responsables de la aplicación del presente capítulo. Los Estados miembros otorgarán a dichas autoridades las competencias necesarias y les proporcionarán los recursos humanos, financieros y técnicos, el equipamiento y los conocimientos necesarios para desempeñar correctamente sus funciones con arreglo al presente Reglamento. Las autoridades de vigilancia del mercado estarán facultadas para adoptar las medidas de vigilancia del mercado a que se refiere el artículo 16 del Reglamento (UE) 2019/1020 con el fin de hacer cumplir las obligaciones establecidas en el presente capítulo. Los Estados miembros comunicarán a la Comisión la identidad de las autoridades de vigilancia del mercado que designen. La Comisión y los Estados miembros pondrán dicha información a disposición del público.

3. Las autoridades de vigilancia del mercado designadas con arreglo al apartado 2 del presente artículo podrán ser las mismas autoridades que las autoridades de salud digital designadas con arreglo al artículo 19. Cuando una autoridad de salud digital desempeñe las funciones de una autoridad de vigilancia del mercado, los Estados miembros se asegurarán de que se evite todo conflicto de intereses.

4. Las autoridades de vigilancia del mercado informarán anualmente a la Comisión sobre los resultados de las actividades pertinentes de vigilancia del mercado.

5. Cuando el fabricante u otro operador económico no coopere con una autoridad de vigilancia del mercado o cuando la información y documentación proporcionadas sean incompletas o incorrectas, la autoridad de vigilancia del mercado podrá adoptar todas las medidas adecuadas para prohibir o restringir la comercialización del sistema HCE pertinente hasta que el fabricante u operador económico de que se trate coopere o proporcione información completa y correcta, o para recuperar o retirar dicho sistema HCE del mercado.

6. Las autoridades de vigilancia del mercado de los Estados miembros cooperarán entre sí y con la Comisión. La Comisión deberá posibilitar que se organicen los intercambios de información necesarios para tal cooperación.

7. En el caso de los productos sanitarios, los productos sanitarios para diagnóstico *in vitro* o los sistemas de IA de alto riesgo a que se refiere el artículo 27, apartados 1 y 2, las autoridades responsables de la vigilancia del mercado serán las mencionadas en el artículo 93 del Reglamento (UE) 2017/745, en el artículo 88 del Reglamento (UE) 2017/746 o en el artículo 70 del Reglamento (UE) 2024/1689, según proceda.

Artículo 44

Gestión de los riesgos que entrañan los sistemas HCE y de los incidentes graves

1. Cuando una autoridad de vigilancia del mercado de un Estado miembro tenga motivos para creer que un sistema HCE entraña un riesgo para la salud, la seguridad o los derechos de las personas físicas o para la protección de datos personales, dicha autoridad de vigilancia del mercado evaluará el sistema HCE en cuestión con respecto a todos los requisitos pertinentes establecidos en el presente Reglamento. El fabricante, su representante autorizado y todos los demás operadores económicos pertinentes cooperarán en la medida necesaria con la autoridad de vigilancia del mercado a tal efecto y adoptarán las medidas adecuadas para asegurarse de que el sistema HCE en cuestión ya no entrañe ese riesgo cuando se introduzca en el mercado, para recuperarlo o para retirarlo del mercado en un plazo razonable.

2. Cuando las autoridades de vigilancia del mercado de un Estado miembro consideren que el incumplimiento del sistema HCE no se limita a su territorio nacional, informarán a la Comisión y a las autoridades de vigilancia del mercado de los demás Estados miembros de los resultados de la evaluación a que se refiere el apartado 1 del presente artículo y de la medida correctiva que hayan pedido al operador económico que adopte con arreglo al artículo 16, apartado 2, del Reglamento (UE) 2019/1020.

3. Cuando una autoridad de vigilancia del mercado considere que un sistema HCE ha causado perjuicios a la salud o la seguridad de las personas físicas o a determinados aspectos relacionados con la protección del interés público, el fabricante proporcionará de inmediato información y documentación, según proceda, a la persona física o usuario afectado por dicho perjuicio y, en su caso, a otros terceros afectados por dicho perjuicio, sin perjuicio de lo dispuesto en la normativa de protección de datos.

4. El operador económico de que se trate a que se refiere el apartado 1 se asegurará de que se adopten medidas correctivas en relación con todos los sistemas HCE afectados que haya introducido en el mercado de la Unión.

5. La autoridad de vigilancia del mercado informará sin demora indebida a la Comisión y a las autoridades de vigilancia del mercado —o, en su caso, a las autoridades de control con arreglo al Reglamento (UE) 2016/679— de los demás Estados miembros de la medida correctiva a que se refiere el apartado 2. Dicha información incluirá todos los detalles disponibles, en particular los datos necesarios para identificar el sistema HCE afectado y para determinar su origen, la cadena de suministro del sistema, el tipo de riesgo planteado y la naturaleza y duración de las medidas nacionales adoptadas.

6. Cuando una constatación de una autoridad de vigilancia del mercado, o un incidente grave del que se le informe, se refiera a la protección de datos personales, dicha autoridad de vigilancia del mercado informará sin demora indebida a las autoridades de control pertinentes con arreglo al Reglamento (UE) 2016/679 y cooperará con ellas.

7. Los fabricantes de sistemas HCE introducidos en el mercado o puestos en servicio notificarán cualquier incidente grave que afecte a un sistema HCE a las autoridades de vigilancia del mercado de los Estados miembros en los que se haya producido dicho incidente grave y de los Estados miembros en los que se hayan introducido o puesto en servicio esos sistemas HCE. Esa notificación incluirá también una descripción de la medida correctiva adoptada o prevista por el fabricante. Los Estados miembros podrán disponer que los usuarios de los sistemas HCE introducidos en el mercado o puestos en servicio puedan notificar tales incidentes.

La notificación que se exige con arreglo al párrafo primero del presente apartado se efectuará, sin perjuicio de los requisitos de notificación de incidentes en virtud de la Directiva (UE) 2022/2555, inmediatamente después de que el fabricante haya establecido un vínculo causal entre el sistema HCE y el incidente grave, o la posibilidad razonable de que exista dicho vínculo, y, en cualquier caso, a más tardar tres días después de que el fabricante tenga conocimiento del incidente grave que afecta al sistema HCE.

8. Las autoridades de vigilancia del mercado a que se refiere el apartado 7 informarán sin demora a las demás autoridades de vigilancia del mercado del incidente grave y de la medida correctiva adoptada o prevista por el fabricante o que se requiera para minimizar el riesgo de que se repita el incidente grave.

9. Cuando la autoridad de salud digital no desempeñe funciones de autoridad de vigilancia del mercado, la autoridad de vigilancia del mercado cooperará con la autoridad de salud digital. La autoridad de vigilancia del mercado informará a la autoridad de salud digital de cualquier incidente grave y de los sistemas HCE que presenten un riesgo, incluidos los riesgos relacionados con la interoperabilidad, la protección y la seguridad de los pacientes, así como de cualquier medida correctiva, y de cualquier recuperación o retirada de dichos sistemas HCE.

10. En caso de incidentes que supongan un riesgo para la seguridad de los pacientes o la seguridad de la información, las autoridades de vigilancia del mercado podrán adoptar medidas inmediatas y requerir al fabricante de sistemas HCE de que se trate, su representante autorizado y otros operadores económicos, según proceda, que adopte medidas correctivas inmediatas.

Artículo 45

Gestión de los casos de incumplimiento

1. Si una autoridad de vigilancia del mercado constata algún caso de incumplimiento, requerirá al fabricante del sistema HCE afectado, a su representante autorizado y a todos los demás operadores económicos pertinentes que adopten, en un plazo determinado, las medidas correctivas adecuadas para poner en conformidad el sistema HCE. En dichas constataciones de incumplimiento se incluirán, sin ser exhaustivos, los siguientes:

a) el sistema HCE no es conforme con los requisitos esenciales establecidos en el anexo II o con las especificaciones comunes a que se refiere el artículo 36;

b) la documentación técnica no está disponible, es incompleta o no es conforme con el artículo 37;

c) la declaración UE de conformidad no se ha elaborado o no se ha elaborado correctamente con arreglo al artículo 39;

d) el marcado CE de conformidad se ha colocado incumpliendo el artículo 41 o no se ha colocado;

e) las obligaciones de registro previstas en el artículo 49 no se han cumplido.

2. Si el fabricante del sistema HCE afectado, su representante autorizado o cualquier otro operador económico pertinente no adoptase las medidas correctivas adecuadas en un plazo razonable, las autoridades de vigilancia del mercado adoptarán todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del sistema HCE en el mercado de sus Estados miembros, o para recuperarlo o retirarlo de ese mercado.

Las autoridades de vigilancia del mercado informarán sin demora de tales medidas provisionales a la Comisión y a las autoridades de vigilancia del mercado de los demás Estados miembros. Esta información incluirá todos los detalles disponibles, en particular los datos necesarios para la identificación del sistema HCE en incumplimiento, su origen, la naturaleza del supuesto incumplimiento y el riesgo planteado, la naturaleza y duración de las medidas adoptadas por las autoridades de vigilancia del mercado y los argumentos expresados por el operador económico correspondiente. En concreto, las autoridades de vigilancia del mercado indicarán si el incumplimiento se debe a cualquiera de los motivos siguientes:

a) el sistema HCE no cumple los requisitos esenciales establecidos en el anexo II;

b) existen deficiencias en cuanto a las especificaciones comunes a que se refiere el artículo 36.

3. Las autoridades de vigilancia del mercado distintas de las autoridades de vigilancia del mercado que iniciaron el procedimiento con arreglo al presente artículo informarán sin demora a la Comisión y a las autoridades de vigilancia del mercado de los demás Estados miembros de toda medida que adopten, de cualquier información adicional de que dispongan sobre el incumplimiento del sistema HCE en cuestión y, en caso de desacuerdo con la medida nacional adoptada, presentarán sus objeciones al respecto.

4. Si, en el plazo de tres meses a partir de la recepción de la información a que se refiere el párrafo segundo del apartado 2, ninguna autoridad de vigilancia del mercado de otro Estado miembro ni la Comisión presentan objeciones en relación con una medida provisional adoptada por una autoridad de vigilancia del mercado, dicha medida se considerará justificada.

5. Si el incumplimiento al que se refiere el apartado 1 persiste, la autoridad de vigilancia del mercado en cuestión adoptará las medidas adecuadas para prohibir o restringir la comercialización del sistema HCE, o garantizará su recuperación o retirada del mercado.

Artículo 46

Procedimiento de salvaguardia de la Unión

1. Si, en virtud del artículo 44, apartado 2, y del artículo 45, apartado 3, se presentasen objeciones contra una medida nacional adoptada por una autoridad de vigilancia del mercado, o si la Comisión considerase que una medida nacional es contraria al Derecho de la Unión, la Comisión consultará sin demora a dicha autoridad de vigilancia del mercado y a los operadores económicos en cuestión, y evaluará la medida nacional de que se trate. Sobre la base de los resultados de esa evaluación, la Comisión adoptará una decisión de ejecución por la que se determine si la medida nacional está justificada. Dicha decisión de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2. La Comisión destinará su decisión de ejecución a todos los Estados miembros y la comunicará inmediatamente a estos y a los operadores económicos correspondientes.

2. Si la Comisión considera que la medida nacional a que se refiere el apartado 1 está justificada, todos los Estados miembros de que se trate adoptarán las medidas necesarias para garantizar que el sistema HCE en incumplimiento sea retirado de sus mercados nacionales, e informarán a la Comisión en consecuencia.

Si la Comisión considera que la medida nacional a que se refiere el apartado 1 no está justificada, el Estado miembro de que se trate la revocará.

SECCIÓN 5

Otras disposiciones sobre interoperabilidad

Artículo 47

Etiquetado de las aplicaciones de bienestar

1. Cuando un fabricante de una aplicación de bienestar declare la interoperabilidad con un sistema HCE en relación con sus componentes armonizados de programa informático y, por tanto, el cumplimiento de las especificaciones comunes a que se refiere el artículo 36 y de los requisitos esenciales establecidos en el anexo II, esa aplicación de bienestar irá acompañada de una etiqueta que indique claramente su conformidad con dichas especificaciones y requisitos. Dicha etiqueta será expedida por el fabricante de la aplicación de bienestar.

2. La etiqueta a que se refiere el apartado 1 incluirá la información siguiente:

a) las categorías de datos de salud electrónicos respecto de las cuales se haya confirmado el cumplimiento de los requisitos esenciales establecidos en el anexo II;

b) una referencia a las especificaciones comunes para demostrar la conformidad;

c) el período de validez de la etiqueta.

3. La Comisión determinará, mediante actos de ejecución, el formato y el contenido de la etiqueta a que se refiere el apartado 1. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

4. La etiqueta se redactará en una o varias lenguas oficiales de la Unión o en una lengua de fácil comprensión que determine el Estado miembro en el que la aplicación de bienestar se introduzca en el mercado o se ponga en servicio.

5. La validez de la etiqueta no excederá de tres años.

6. Si la aplicación de bienestar es una parte integrante de un dispositivo o es integrada en un dispositivo después de que haya sido puesto en servicio, la etiqueta que la acompaña figurará en la propia aplicación o se colocará sobre ese dispositivo. Cuando la aplicación de bienestar consista solamente en un programa informático, la etiqueta tendrá un formato digital y figurará en la propia aplicación. También podrán utilizarse códigos de barras bidimensionales (2D) para mostrar la etiqueta.

7. Las autoridades de vigilancia del mercado comprobarán la conformidad de las aplicaciones de bienestar con los requisitos esenciales establecidos en el anexo II.

8. Cada proveedor de una aplicación de bienestar para la que se haya expedido una etiqueta garantizará que la aplicación que se introduzca en el mercado o se ponga en servicio vaya acompañada gratuitamente de la etiqueta para cada unidad individual.

9. Cada distribuidor de una aplicación de bienestar para la que se haya expedido una etiqueta la pondrá a disposición de los clientes en el punto de venta en formato electrónico.

Artículo 48

Interoperabilidad de las aplicaciones de bienestar con los sistemas HCE

1. Los fabricantes de aplicaciones de bienestar podrán declarar la interoperabilidad de estas con un sistema HCE siempre que se cumplan las especificaciones comunes y los requisitos esenciales a que se refieren el artículo 36 y el anexo II, respectivamente. En los casos en que esta declaración se realice, los fabricantes informarán debidamente a los usuarios de la interoperabilidad de dichas aplicaciones de bienestar y de los efectos de dicha interoperabilidad.

2. La interoperabilidad de las aplicaciones de bienestar con los sistemas HCE no supondrá que la totalidad o parte de los datos de salud de la aplicación de bienestar se intercambien automáticamente con el sistema HCE o se transmitan automáticamente al sistema. El intercambio o la transmisión de dichos datos solo serán posibles si se hace con arreglo al artículo 5 y previo consentimiento de la persona física de que se trate, y la interoperabilidad se limitará exclusivamente a esos fines. Los fabricantes de aplicaciones de bienestar que declaren la interoperabilidad de estas con un sistema HCE garantizarán que la persona física de que se trate pueda escoger qué categorías de datos de salud de la aplicación de bienestar vayan a introducirse en el sistema HCE y las circunstancias en que se realice el intercambio o transmisión de dichas categorías de datos.

SECCIÓN 6

Registro de los sistemas HCE y las aplicaciones de bienestar

Artículo 49

Base de datos de la UE para el registro de los sistemas HCE y las aplicaciones de bienestar

1. La Comisión creará y mantendrá una base de datos de la UE de acceso público con datos sobre los sistemas HCE para los que se haya emitido una declaración UE de conformidad con arreglo al artículo 39 y las aplicaciones de bienestar para las que se haya expedido una etiqueta con arreglo al artículo 47 (en lo sucesivo, «base de datos de la UE para el registro de los sistemas HCE y las aplicaciones de bienestar»).

2. Antes de introducir en el mercado o poner en servicio un sistema HCE a que se refiere el artículo 26 o una aplicación de bienestar a que se refiere el artículo 47, el fabricante de dicho sistema HCE o de dicha aplicación de bienestar o, en su caso, su representante autorizado, introducirá los datos requeridos a que se refiere el apartado 4 del presente artículo, en la base de datos de la UE para el registro de los sistemas HCE y las aplicaciones de bienestar, incluidos, en el caso de los sistemas HCE, los resultados de la evaluación a que se refiere el artículo 40.

3. Los productos sanitarios, los productos sanitarios para diagnóstico *in vitro* o los sistemas de IA de alto riesgo a que se refiere el artículo 27, apartados 1 y 2, del presente Reglamento también se registrarán en las bases de datos creadas de conformidad con los Reglamentos (UE) 2017/745, (UE) 2017/746 o (UE) 2024/1689, según proceda. En tales casos, los datos que se deban introducir también se transmitirán a la base de datos de la UE para el registro de los sistemas HCE y las aplicaciones de bienestar.

4. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 97 para completar el presente Reglamento mediante la determinación de la lista de los datos que deben introducir los fabricantes de sistemas HCE en la base de datos de la UE para el registro de los sistemas HCE y las aplicaciones de bienestar con arreglo al apartado 2 del presente artículo.

CAPÍTULO IV

USO SECUNDARIO

SECCIÓN 1

Condiciones generales relativas al uso secundario

Artículo 50

Aplicabilidad a los tenedores de datos de salud

1. Las siguientes categorías de tenedores de datos de salud estarán exentas de las obligaciones de los tenedores de datos de salud establecidas en el presente capítulo:

a) las personas físicas, incluidos los investigadores individuales;

b) las personas jurídicas que puedan considerarse microempresas tal como se definen en el artículo 2, apartado 3, del anexo de la Recomendación 2003/361/CE.

2. Los Estados miembros podrán disponer en su Derecho nacional que las obligaciones de los tenedores de datos de salud establecidas en el presente capítulo se apliquen a los tenedores de datos de salud a que se refiere el apartado 1 que estén bajo su jurisdicción.

3. Los Estados miembros podrán disponer en su Derecho nacional que las obligaciones de determinadas categorías de tenedores de datos de salud sean asumidas por entidades de intermediación de datos de salud. En ese caso, los datos se considerarán, no obstante, puestos a disposición por varios tenedores de datos de salud.

4. Los Estados miembros notificarán a la Comisión las medidas de Derecho nacional a que se refieren los apartados 2 y 3 a más tardar el 26 de marzo de 2029. Toda normativa nueva o modificación posterior que afecte a esas medidas se notificará sin demora a la Comisión.

Artículo 51

Categorías mínimas de datos de salud electrónicos para uso secundario

1. Los tenedores de datos de salud pondrán a disposición las siguientes categorías de datos de salud electrónicos para uso secundario de conformidad con lo dispuesto en el presente capítulo:

a) datos de salud electrónicos procedentes de HCE;

b) datos sobre factores que influyen en la salud, incluidos los socioeconómicos, ambientales y de comportamiento determinantes para la salud;

c) datos agregados sobre las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la prestación de asistencia sanitaria y el acceso a la misma, el gasto de asistencia sanitaria y su financiación;

d) datos sobre patógenos que influyen en la salud humana;

e) datos administrativos relacionados con la asistencia sanitaria, incluidos los datos sobre dispensación, solicitudes de reembolso y reembolsos;

f) datos genéticos, epigenómicos y genómicos humanos;

g) otros datos moleculares humanos, como datos proteómicos, transcriptómicos, metabolómicos, lipidómicos y otros datos ómicos;

h) datos de salud electrónicos personales generados automáticamente mediante productos sanitarios;

i) datos procedentes de aplicaciones de bienestar;

j) datos sobre la situación profesional, la especialización y el establecimiento de los profesionales sanitarios que dispensan tratamiento a una persona física;

k) datos procedentes de registros de datos de salud de base poblacional (como, por ejemplo, registros de salud pública);

l) datos procedentes de los registros médicos y los registros de mortalidad;

m) datos procedentes de ensayos clínicos, estudios clínicos, investigaciones clínicas y estudios de rendimiento a los que se aplica el Reglamento (UE) n.º 536/2014, el Reglamento (UE) 2024/1938 del Parlamento Europeo y del Consejo ([35]), el Reglamento (UE) 2017/745 o el Reglamento (UE) 2017/746;

n) otros datos de salud procedentes de productos sanitarios;

o) datos procedentes de los registros de medicamentos y productos sanitarios;

p) datos procedentes de grupos de investigación, cuestionarios y encuestas relacionadas con la salud, tras la primera publicación de los resultados correspondientes;

q) datos de salud procedentes de biobancos y bases de datos asociadas.

2. Los Estados miembros podrán disponer en su Derecho nacional que se pongan a disposición categorías adicionales de datos de salud electrónicos para uso secundario con arreglo al presente Reglamento.

3. Los Estados miembros podrán establecer reglas para el tratamiento y el uso de datos de salud electrónicos que contengan mejoras relacionadas con el tratamiento de dichos datos —como la corrección, la anotación y el enriquecimiento — sobre la base de un permiso de datos con arreglo al artículo 68.

4. Los Estados miembros podrán introducir medidas más estrictas y garantías adicionales a nivel nacional destinadas a salvaguardar la sensibilidad y el valor de los datos contemplados en el apartado 1, letras f), g), i) y q). Los Estados miembros notificarán dichas medidas y garantías a la Comisión y, sin demora, toda modificación posterior.

Artículo 52

Derechos de propiedad intelectual e industrial y secretos comerciales

1. Los datos de salud electrónicos protegidos por derechos de propiedad intelectual e industrial o secretos comerciales o amparados por el derecho de protección reglamentaria de los datos previsto en el artículo 10, apartado 1, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo ([36]) o en el artículo 14, apartado 11, del Reglamento (CE) n.º 726/2004 del Parlamento Europeo y del Consejo ([37]) se pondrán a disposición para su uso secundario de conformidad con lo dispuesto en el presente Reglamento.

2. Los tenedores de datos de salud informarán al organismo de acceso a datos de salud sobre cualesquiera datos de salud electrónicos que incluyan contenidos o información protegidos por derechos de propiedad intelectual e industrial o secretos comerciales o amparados por el derecho de protección legal de los datos previsto en el artículo 10, apartado 1, de la

([35]) Reglamento (UE) 2024/1938 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, sobre las normas de calidad y seguridad de las sustancias de origen humano destinadas a su aplicación en el ser humano y por el que se derogan las Directivas 2002/98/CE y 2004/23/CE (DO L, 2024/1938, 17.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1938/oj).

([36]) Directiva 2001/83/CE del Parlamento Europeo y del Consejo, de 6 de noviembre de 2001, por la que se establece un código comunitario sobre medicamentos para uso humano (DO L 311 de 28.11.2001, p. 67).

([37]) Reglamento (CE) n.º 726/2004 del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, por el que se establecen procedimientos de la Unión para la autorización y el control de los medicamentos de uso humano y por el que se crea la Agencia Europea de Medicamentos (DO L 136 de 30.4.2004, p. 1).

Directiva 2001/83/CE o en el artículo 14, apartado 11, del Reglamento (CE) n.º 726/2004. Los tenedores de datos de salud indicarán qué partes de los conjuntos de datos se ven afectadas y justificarán la necesidad de protección específica de los datos. Los tenedores de datos de salud proporcionarán dicha información al comunicar al organismo de acceso a datos de salud las descripciones de los conjuntos de datos en su poder con arreglo al artículo 60, apartado 3, del presente Reglamento o, a más tardar, cuando así lo solicite el organismo de acceso a datos de salud.

3. Los organismos de acceso a datos de salud adoptarán todas las medidas específicas adecuadas y proporcionadas —incluidas medidas de naturaleza jurídica, organizativa y técnica— que consideren necesarias para proteger los derechos de propiedad intelectual e industrial, los secretos comerciales o el derecho de protección legal de los datos previsto en el artículo 10, apartado 1, de la Directiva 2001/83/CE o en el artículo 14, apartado 11, del Reglamento (CE) n.º 726/2004. Seguirá correspondiendo a los organismos de acceso a datos de salud determinar la necesidad e idoneidad de dichas medidas.

4. Al expedir permisos de datos con arreglo al artículo 68, los organismos de acceso a datos de salud podrán supeditar el acceso a determinados datos de salud electrónicos a medidas jurídicas, organizativas y técnicas, que podrán incluir acuerdos contractuales entre los tenedores de datos de salud y los usuarios de datos de salud con el fin de intercambiar datos que contengan información o contenidos protegidos por derechos de propiedad intelectual e industrial o secretos comerciales. La Comisión elaborará y recomendará cláusulas contractuales tipo no vinculantes para dichos acuerdos.

5. En caso de que la concesión de acceso a datos de salud electrónicos para uso secundario conlleve un riesgo grave —al que no pueda hacerse frente satisfactoriamente— de vulnerar derechos de propiedad intelectual e industrial, secretos comerciales o el derecho de protección legal de los datos previsto en el artículo 10, apartado 1, de la Directiva 2001/83/CE o en el artículo 14, apartado 11, del Reglamento (CE) n.º 726/2004, el organismo de acceso a datos de salud denegará al solicitante de datos de salud el acceso a dichos datos. El organismo de acceso a datos de salud informará al solicitante de datos de salud de esta denegación y le proporcionará una justificación a este respecto. Los tenedores de datos de salud y los solicitantes de datos de salud tendrán derecho a presentar una reclamación de conformidad con el artículo 81 del presente Reglamento.

Artículo 53

Fines para los que pueden tratarse datos de salud electrónicos para uso secundario

1. Los organismos de acceso a datos de salud solo concederán a un usuario de datos de salud acceso a los datos de salud electrónicos a que se refiere el artículo 51 para uso secundario cuando el tratamiento de los datos por ese usuario de datos de salud sea necesario para alguno de los fines siguientes:

a) el interés público en el ámbito de la salud pública o la salud laboral, por ejemplo actividades destinadas a la protección contra las amenazas transfronterizas graves para la salud, la vigilancia de la salud pública o actividades destinadas a garantizar unos niveles elevados de calidad y seguridad de la asistencia sanitaria, incluida la seguridad de los pacientes, y de los medicamentos o productos sanitarios;

b) las actividades de formulación de políticas y de regulación en apoyo a los organismos del sector público o a las instituciones, órganos u organismos de la Unión, incluidas las autoridades reguladoras, en el sector sanitario o en el sector asistencial en el desempeño de las funciones definidas en sus mandatos;

c) las estadísticas tal como se definen en el artículo 3, punto 1, del Reglamento (CE) n.º 223/2009 como, por ejemplo, las estadísticas oficiales nacionales, plurinacionales y de la Unión relativas al sector sanitario o en el sector asistencial;

d) las actividades de educación o de enseñanza en el sector sanitario o asistencial a nivel de formación profesional o educación superior;

e) la investigación científica relacionada con el sector sanitario o asistencial que contribuya a la salud pública o a la evaluación de tecnologías sanitarias o que procure niveles elevados de calidad y seguridad de la asistencia sanitaria, de los medicamentos o de los productos sanitarios, con el objetivo de beneficiar a los usuarios finales, como los pacientes, los profesionales sanitarios y los administradores sanitarios, lo que incluye:

   i) las actividades de desarrollo e innovación para productos o servicios,

   ii) el entrenamiento, la prueba y la evaluación de algoritmos, también con respecto a productos sanitarios, productos sanitarios para diagnóstico *in vitro*, sistemas de IA y aplicaciones sanitarias digitales;

f) la mejora de la prestación de asistencia, la optimización de los tratamientos y la prestación de asistencia sanitaria, sobre la base de los datos de salud electrónicos de otras personas físicas.

2. El acceso a los datos de salud electrónicos para los fines mencionados en el apartado 1, letras a) a c), estará reservado a los organismos del sector público y a las instituciones, órganos y organismos de la Unión que ejerzan las misiones que les confiere el Derecho de la Unión o nacional, también cuando el tratamiento de datos para desempeñar esas misiones se encomiende a un tercero en nombre de dichos organismos del sector público o de las instituciones, órganos y organismos de la Unión.

Artículo 54

Uso secundario prohibido

Los usuarios de datos de salud solo tratarán datos de salud electrónicos para uso secundario sobre la base y de acuerdo con los fines que figuren en un permiso de datos expedido con arreglo al artículo 68, peticiones de datos de salud aprobadas con arreglo al artículo 69 o, en las situaciones a que se refiere el artículo 67, apartado 3, una aprobación de acceso por parte del correspondiente participante autorizado en DatosSalud@UE a que se refiere el artículo 75.

En particular, queda prohibido el acceso y el tratamiento de los datos de salud electrónicos obtenidos a través de un permiso de datos expedido con arreglo al artículo 68 o de una petición de datos aprobada con arreglo al artículo 69 cuando la finalidad de uso sea:

a) tomar decisiones perjudiciales para una persona física o un grupo de personas físicas sobre la base de sus datos de salud electrónicos; para ser calificadas de «decisiones» a efectos de la presente letra, deben producir efectos jurídicos, económicos o sociales, o afectar de manera igualmente significativa a dichas personas físicas;

b) tomar decisiones en relación con una persona física o un grupo de personas físicas por lo que respecta a ofertas de empleo, ofrecerles condiciones menos favorables en la provisión de bienes o servicios, incluida la exclusión de dichas personas o grupos del beneficio de un contrato de seguro o de crédito, la modificación de sus cotizaciones y primas de seguro o condiciones de préstamo, o tomar cualquier otra decisión respecto de una persona física o un grupo de personas físicas que resulte en una discriminación contra ellos sobre la base de los datos de salud obtenidos;

c) realizar actividades de publicidad o mercadotecnia;

d) desarrollar productos o servicios que puedan perjudicar a las personas, a la salud pública o a la sociedad en general, por ejemplo, drogas ilegales, bebidas alcohólicas, productos del tabaco y nicotina, armamento o productos o servicios diseñados o modificados de manera que creen adicción, contravengan el orden público o pongan en riesgo la salud humana;

e) realizar actividades que entren en conflicto con disposiciones de Derecho nacional en materia de ética;

SECCIÓN 2

Gobernanza y mecanismos para uso secundario

Artículo 55

Organismos de acceso a datos de salud

1. Los Estados miembros designarán uno o varios organismos de acceso a datos de salud responsables de cumplir las funciones y obligaciones establecidas en los artículos 57, 58 y 59. Los Estados miembros podrán crear uno o varios nuevos organismos del sector público o recurrir a organismos del sector público existentes o a servicios internos de organismos del sector público que cumplan las condiciones establecidas en el presente artículo. Las funciones establecidas en el artículo 57 podrán repartirse entre diferentes organismos de acceso a datos de salud. Cuando un Estado miembro designe varios organismos de acceso a datos de salud, elegirá a uno de ellos para actuar como coordinador, con la responsabilidad de coordinar las funciones con los demás organismos de acceso a datos de salud, tanto en el territorio de ese Estado miembro como en los demás Estados miembros.

Todos los organismos de acceso a datos de salud contribuirán a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, los organismos de acceso a datos de salud cooperarán entre sí, con la Comisión y, por lo que respecta a cuestiones relacionadas con la protección de datos, con las autoridades de control pertinentes.

2. A fin de contribuir al desempeño efectivo de las funciones y al ejercicio de las competencias de los organismos de acceso a datos de salud, los Estados miembros garantizarán que cada organismo de acceso a datos de salud disponga de los elementos siguientes:

a) los recursos humanos, financieros y técnicos necesarios;

b) los conocimientos especializados necesarios, y

b) los locales e infraestructuras necesarios.

Cuando el Derecho nacional exija una evaluación por parte de organismos de ética, dichos organismos pondrán sus conocimientos especializados a disposición del organismo de acceso a datos de salud. Como alternativa, los Estados miembros podrán disponer que organismos de ética formen parte del organismo de acceso a datos de salud.

3. Los Estados miembros garantizarán que se evite cualquier conflicto de intereses entre las partes organizativas de los organismos de acceso a datos de salud que desempeñen las diferentes funciones de dichos organismos, por ejemplo mediante el establecimiento de garantías organizativas, como la segregación entre las diferentes funciones de los organismos de acceso a datos de salud, incluido entre la evaluación de las solicitudes, la recepción y preparación de los conjuntos de datos —como, por ejemplo, la anonimización y seudonimización de conjuntos de datos— y el suministro de los datos en entornos de tratamiento seguros.

4. En el desempeño de sus funciones, los organismos de acceso a datos de salud cooperarán activamente con los representantes de las partes interesadas pertinentes, especialmente con los representantes de los pacientes, los tenedores de datos de salud y los usuarios de datos de salud, y evitarán todo conflicto de intereses.

5. En el desempeño de sus funciones y en el ejercicio de sus competencias, los organismos de acceso a datos de salud evitarán cualquier conflicto de intereses. El personal de los organismos de acceso a datos de salud actuará en favor del interés público y de manera independiente.

6. Los Estados miembros informarán a la Comisión sobre la identidad de los organismos de acceso a datos de salud designados con arreglo al apartado 1 a más tardar el 26 de marzo de 2027. Asimismo, informarán a la Comisión sobre toda modificación posterior de la identidad de dichos organismos. La Comisión y los Estados miembros pondrán dicha información a disposición del público.

Artículo 56

Servicio de acceso a datos de salud de la Unión

1. La Comisión ejercerá las funciones establecidas en los artículos 57 y 59 cuando los tenedores de datos de salud sean instituciones, órganos u organismos de la Unión.

2. La Comisión se asegurará de que se asignen los recursos humanos, técnicos y financieros, así como los locales y las infraestructuras, que resulten necesarios para el desempeño efectivo de las funciones establecidas en los artículos 57 y 59 y para el ejercicio de sus funciones.

3. Salvo que se excluya de manera explícita, las referencias a los organismos de acceso a datos de salud contenidas en el presente Reglamento en relación con el desempeño de las funciones y el ejercicio de sus funciones se entenderán también aplicables a la Comisión cuando los tenedores de datos de salud sean instituciones, órganos u organismos de la Unión.

Artículo 57

Funciones de los organismos de acceso a datos de salud

1. Los organismos de acceso a datos de salud desempeñarán las funciones siguientes:

a) decidir sobre las solicitudes de acceso a datos de salud con arreglo al artículo 67 del presente Reglamento, autorizar y expedir permisos de datos con arreglo al artículo 68 del presente Reglamento para acceder a los datos de salud electrónicos para uso secundario que sean de su competencia y decidir sobre las peticiones de datos de salud presentadas con arreglo al artículo 69 del presente Reglamento, de conformidad con el presente capítulo y con el capítulo II del Reglamento (UE) 2022/868, entre otros, por lo que respecta a lo siguiente:

   i) proporcionar a los usuarios de datos de salud acceso a los datos de salud electrónicos con arreglo a un permiso de datos, en un entorno de tratamiento seguro, de conformidad con los requisitos establecidos en el artículo 73,

   ii) realizar un seguimiento y supervisar el cumplimiento de los requisitos establecidos en el presente Reglamento por parte de los usuarios de datos de salud y de los tenedores de datos de salud,

   iii) solicitar los datos de salud electrónicos a que se refiere el artículo 51 a los tenedores de datos de salud pertinentes con arreglo a un permiso de datos expedido o una petición de datos aprobada;

b) tratar los datos de salud electrónicos a que se refiere el artículo 51, por ejemplo, la recepción, combinación, preparación y recopilación de tales datos cuando así lo soliciten los tenedores de datos de salud y la seudonimización o anonimización de esos datos;

c) adoptar todas las medidas necesarias para preservar la confidencialidad de los derechos de propiedad intelectual e industrial y la protección legal de los datos, así como la confidencialidad de los secretos comerciales con arreglo a lo dispuesto en el artículo 52, teniendo en cuenta los derechos pertinentes tanto del tenedor de datos de salud como del usuario de datos de salud;

d) cooperar con los tenedores de datos de salud y supervisarlos para garantizar la aplicación coherente y precisa de las disposiciones en materia de etiqueta de calidad y utilidad de los datos del artículo 78;

e) mantener un sistema de gestión para registrar y tramitar las solicitudes de acceso a datos de salud, las peticiones de datos de salud, las decisiones sobre esas solicitudes y peticiones y los permisos de datos expedidos y las peticiones de datos de salud atendidas, proporcionando como mínimo información sobre el nombre del solicitante de datos de salud, la finalidad del acceso, la fecha de expedición, la duración del permiso de datos y una descripción de la solicitud de acceso a datos de salud o de la petición de datos de salud;

f) mantener un sistema de información pública para cumplir las obligaciones establecidas en el artículo 58;

g) cooperar a escala nacional y de la Unión para establecer normas comunes, requisitos técnicos y medidas adecuadas para acceder a los datos de salud electrónicos en un entorno de tratamiento seguro;

h) cooperar a escala nacional y de la Unión y asesorar a la Comisión sobre técnicas y mejores prácticas para el uso secundario y la gestión de datos de salud electrónicos;

i) facilitar el acceso transfronterizo a los datos de salud electrónicos para uso secundario alojados en otros Estados miembros a través de DatosSalud@UE a que se refiere el artículo 75 y cooperar estrechamente entre sí y con la Comisión;

j) publicar, por medios electrónicos:

   i) un catálogo nacional de conjuntos de datos que incluya detalles sobre la fuente y la naturaleza de los datos de salud electrónicos, de conformidad con los artículos 77, 78 y 80, y las condiciones para su puesta a disposición,

   ii) toda solicitud de acceso a datos de salud y petición de datos de salud sin demora injustificada tras su primera recepción,

   iii) todos los permisos de datos expedidos o peticiones de datos de salud que se hayan aprobado, así como todas las decisiones de denegación, junto con su justificación, en el plazo de treinta días hábiles a partir de la expedición, aprobación o denegación,

   iv) las medidas relacionadas con el incumplimiento con arreglo al artículo 63,

   v) los resultados comunicados por los usuarios de datos de salud de conformidad con el artículo 61, apartado 4,

   vi) un sistema de información para cumplir las obligaciones establecidas en el artículo 58,

   vii) información, como mínimo en un sitio o portal web de fácil acceso, sobre la conexión a DatosSalud@UE de los puntos de contacto nacionales para uso secundario de un tercer país, o de un sistema establecido a nivel internacional por una organización internacional, tan pronto como el tercer país o la organización internacional se convierta en un participante autorizado en DatosSalud@UE;

k) cumplir las obligaciones con respecto a las personas físicas con arreglo al artículo 58,

l) desempeñar cualquier otra función relacionada con posibilitar el uso secundario de datos de salud electrónicos en el contexto del presente Reglamento.

El catálogo nacional de conjuntos de datos a que se refiere el punto j), inciso i), del presente apartado también se pondrá a disposición de los puntos únicos de información con arreglo al artículo 8 del Reglamento (UE) 2022/868.

2. En el ejercicio de sus funciones, los organismos de acceso a datos de salud:

a) cooperarán con las autoridades de control del Reglamento (UE) 2016/679 en relación con los datos de salud electrónicos personales y con el Consejo del EEDS;

b) cooperarán con todas las partes interesadas pertinentes, incluidas las organizaciones de pacientes, los representantes de las personas físicas, los profesionales sanitarios, los investigadores y los comités de ética, cuando proceda de conformidad con el Derecho de la Unión o nacional;

c) cooperarán con otros organismos nacionales competentes, incluidas las autoridades nacionales que supervisan a las organizaciones de cesión altruista de datos en virtud del Reglamento (UE) 2022/868, las autoridades competentes en virtud del Reglamento (UE) 2023/2854 y las autoridades nacionales competentes en virtud de los Reglamentos (UE) 2017/745, (UE) 2017/746 y (UE) 2024/1689, según proceda.

3. Los organismos de acceso a datos de salud podrán prestar asistencia a los organismos del sector público cuando estos accedan a datos de salud electrónicos de conformidad con el artículo 14 del Reglamento (UE) 2023/2854.

4. Los organismos de acceso a datos de salud podrán prestar apoyo a un organismo del sector público cuando este obtenga datos en las circunstancias a que se refiere el artículo 15, letras a) o b), del Reglamento (UE) 2023/2854, de conformidad con lo dispuesto en dicho Reglamento, proporcionándole apoyo técnico para el tratamiento de esos datos o para combinarlos con otros datos para su análisis conjunto.

Artículo 58

Obligaciones de los organismos de acceso a datos de salud con respecto a las personas físicas

1. Los organismos de acceso a datos de salud pondrán a disposición del público, de forma que sea de fácil consulta mediante medios electrónicos y accesible para las personas físicas, información sobre las condiciones en las que los datos de salud electrónicos se ponen a disposición para uso secundario. Esa información englobará:

a) la base jurídica en virtud de la cual se concede el acceso a datos de salud electrónicos al usuario de datos de salud;

b) las medidas técnicas y organizativas adoptadas para proteger los derechos de las personas físicas;

c) los derechos de las personas físicas aplicables en relación con el uso secundario;

d) las disposiciones para que las personas físicas ejerzan sus derechos de conformidad con el capítulo III del Reglamento (UE) 2016/679;

e) la identidad y los datos de contacto del organismo de acceso a datos de salud;

f) a quién se ha otorgado acceso a conjuntos de datos de salud electrónicos y a qué conjuntos de datos se ha concedido acceso, y detalles del permiso de datos relativo a los fines del tratamiento de dichos datos a que se refiere el artículo 53, apartado 1;

g) los resultados o los productos de los proyectos para los que se utilizaron los datos de salud electrónicos.

2. Cuando un Estado miembro haya previsto que el derecho de autoexclusión con arreglo al artículo 71 se ejerza mediante los organismos de acceso a datos de salud, los organismos de acceso a datos de salud pertinentes proporcionarán información pública sobre el procedimiento de autoexclusión y facilitarán el ejercicio de ese derecho.

3. Cuando un usuario de datos de salud informe a un organismo de acceso a datos de salud de una constatación significativa relativa al estado de salud de una persona física, tal como se contempla en el artículo 61, apartado 5, el organismo de acceso a datos de salud informará de ello al tenedor de datos de salud. El tenedor de datos de salud, en las condiciones establecidas por el Derecho nacional, informará a la persona física o al profesional sanitario que esté tratando a la persona física afectada. Las personas físicas tendrán derecho a solicitar que no se las informe de tales constataciones.

4. Los Estados miembros informarán al público en general sobre la función y los beneficios de los organismos de acceso a datos de salud.

Artículo 59

Presentación de informes por los organismos de acceso a datos de salud

1. Cada organismo de acceso a datos de salud publicará un informe bienal de actividad y lo pondrá a disposición del público en su sitio web. Cuando un Estado miembro designe más de un organismo de acceso a datos de salud, el organismo coordinador a que se refiere el artículo 55, apartado 1, será responsable del informe de actividad y solicitará la información necesaria a los demás organismos de acceso a datos de salud. Dicho informe de actividad seguirá una estructura acordada en el Consejo del EEDS con arreglo al artículo 94, apartado 2, letra d), e incluirá, como mínimo, las categorías de información siguientes:

a) información relativa a las solicitudes de acceso a datos de salud y peticiones de datos de salud que se hayan presentado, como, por ejemplo, los tipos de solicitantes de datos de salud, el número de permisos de datos expedidos o denegados, las categorías de finalidad de acceso y las categorías de datos de salud electrónicos a los que se haya accedido, así como un resumen de los resultados de los usos de los datos de salud electrónicos, cuando proceda;

b) información sobre el cumplimiento de obligaciones legales o contractuales por los usuarios de datos de salud y los tenedores de datos de salud, así como sobre el número y el importe de las multas administrativas impuestas por los organismos de acceso a datos de salud;

c) información sobre las auditorías realizadas a los usuarios de datos de salud para garantizar que el tratamiento que realicen en el entorno de tratamiento seguro cumple la legalidad con arreglo a lo dispuesto en el artículo 73, apartado 1, letra e);

d) información sobre las auditorías internas y por terceros a que se refiere el artículo 73, apartado 3, relativas a la conformidad de los entornos de tratamiento seguros con las normas, especificaciones, y requisitos definidos;

e) información sobre la tramitación de las peticiones de personas físicas con respecto al ejercicio de sus derechos de protección de datos;

f) una descripción de las actividades del organismo de acceso a datos de salud realizadas en relación con el compromiso con las partes interesadas pertinentes;

g) los ingresos procedentes de permisos de datos y peticiones de datos de salud;

h) el número promedio de días transcurridos entre las solicitudes de acceso a datos de salud o las peticiones de datos de salud y el acceso a los datos;

i) el número de etiquetas de calidad de los datos expedidas por los tenedores de datos de salud, desglosadas por categoría de calidad;

j) el número de publicaciones de investigación revisadas por pares, documentos estratégicos y procedimientos de regulación que utilizan datos a los que se accede a través del EEDS;

k) el número de productos y servicios sanitarios digitales, incluidas las aplicaciones de IA, desarrollados utilizando datos a los que se accede a través del EEDS.

2. El informe de actividad a que se refiere el apartado 1 se presentará a la Comisión y al Consejo del EEDS en un plazo de seis meses a partir del final del segundo año del período de presentación de informes pertinente. Podrá accederse al informe de actividad a través del sitio web de la Comisión.

Artículo 60

Obligaciones de los tenedores de datos de salud

1. Los tenedores de datos de salud pondrán a disposición del organismo de acceso a datos de salud, previa petición, los datos de salud electrónicos pertinentes a que se refiere el artículo 51, de conformidad con un permiso de datos expedido con arreglo al artículo 68 o previa petición de datos de salud aprobada con arreglo al artículo 69.

2. Los tenedores de datos de salud pondrán los datos de salud electrónicos solicitados a que se refiere el apartado 1 a disposición del organismo de acceso a datos de salud en un plazo razonable y, a más tardar, tres meses desde la recepción de la petición del organismo de acceso a datos de salud. En casos justificados, el organismo de acceso a datos de salud podrá prorrogar dicho plazo por un período máximo de tres meses.

3. El tenedor de datos de salud comunicará al organismo de acceso a datos de salud una descripción del conjunto de datos en su poder de conformidad con el artículo 77. El tenedor de datos de salud comprobará, como mínimo una vez al año, que su descripción de los conjuntos de datos en el catálogo de conjuntos de datos nacional es exacta y está actualizada.

4. Cuando una etiqueta de calidad y utilidad de los datos acompañe al conjunto de datos con arreglo al artículo 78, el tenedor de datos de salud aportará documentación suficiente al organismo de acceso a datos de salud para que este pueda verificar la exactitud de la etiqueta.

5. Los tenedores de datos de salud electrónicos no personales proporcionarán acceso a los datos a través de bases de datos abiertas y fiables para garantizar el acceso sin limitaciones a todos los usuarios y el almacenamiento y la conservación de los datos. Las bases de datos públicas abiertas y fiables dispondrán de una gobernanza sólida, transparente y sostenible y de un modelo transparente de acceso de los usuarios.

Artículo 61

Obligaciones de los usuarios de datos de salud

1. Los usuarios de datos de salud podrán acceder a los datos de salud electrónicos a que se refiere el artículo 51 para uso secundario, y tratar dichos datos, solo de conformidad con un permiso de datos expedido con arreglo al artículo 68, una petición de datos de salud aprobada con arreglo al artículo 69 o, en las situaciones a que se refiere el artículo 67, apartado 3, una aprobación de acceso por parte del participante autorizado pertinente en DatosSalud@UE a que se refiere el artículo 75.

2. Cuando traten datos de salud electrónicos en los entornos de tratamiento seguros a que se refiere el artículo 73, los usuarios de datos de salud no podrán proporcionar acceso a los datos de salud electrónicos a terceros no mencionados en el permiso de datos ni poner dichos datos a su disposición.

3. Los usuarios de datos de salud no reidentificarán ni intentarán reidentificar a las personas físicas a que se refieran los datos de salud electrónicos obtenidos por los usuarios de datos de salud en virtud de un permiso de datos, una petición de datos de salud o una aprobación de acceso otorgada por parte de un participante autorizado en DatosSalud@UE.

4. Los usuarios de datos de salud harán públicos los resultados o productos del uso secundario, incluida la información pertinente para la prestación de asistencia sanitaria, en un plazo de dieciocho meses a partir de que se haya completado el tratamiento de los datos de salud electrónicos en el entorno de tratamiento seguro o de haber recibido la respuesta a la petición de datos de salud a que se refiere el artículo 69.

En casos justificados relacionados con los fines permitidos del tratamiento de los datos de salud electrónicos, el organismo de acceso a datos de salud podrá prorrogar el plazo a que se refiere el párrafo primero, en particular en los casos en que el resultado se publique en una revista científica u otra publicación científica.

Los resultados o productos del uso secundario solo contendrán datos anonimizados.

Los usuarios de datos de salud informarán de los resultados y productos del uso secundario a los organismos de acceso a datos de salud de los que hayan obtenido el permiso de datos y les prestarán asistencia para que esa información sea pública en los sitios web de los organismos de acceso a datos de salud. Dicha publicación se entenderá sin perjuicio de los derechos de publicación en revistas científicas u otras publicaciones científicas.

Cuando los usuarios de datos de salud utilicen datos de salud electrónicos de conformidad con el presente capítulo, indicarán las fuentes de los datos de salud electrónicos y el hecho de que estos se han obtenido en el marco del EEDS.

5. Sin perjuicio de lo dispuesto en el apartado 2, los usuarios de datos de salud informarán al organismo de acceso a datos de salud de cualquier hallazgo significativo relacionado con la salud de la persona física cuyos datos estén incluidos en el conjunto de datos.

6. Los usuarios de datos de salud cooperarán con los organismos de acceso a datos de salud en el desempeño de las funciones de dichos organismos.

Artículo 62

Tasas

1. Los organismos de acceso a datos de salud, incluido el servicio de acceso de datos de salud de la Unión, o los tenedores fiables de datos de salud a que se refiere el artículo 72, podrán cobrar tasas por la puesta a disposición de datos de salud electrónicos para uso secundario.

Las tasas serán proporcionales al coste de puesta a disposición de los datos y no limitarán la competencia.

Las tasas cubrirán total o parcialmente los costes relacionados con el procedimiento de evaluación de la solicitud de acceso a datos de salud o la petición de datos de salud, de expedición, denegación o modificación de un permiso de datos con arreglo a los artículos 67 y 68, o de respuesta a una petición de datos de salud presentada con arreglo al artículo 69, incluidos los costes relacionados con la consolidación, preparación, seudonimización, anonimización y suministro de los datos de salud electrónicos.

Los Estados miembros podrán fijar tasas reducidas para determinados tipos de usuarios de datos de salud situados en la Unión, como los organismos del sector público o instituciones, órganos y organismos de la Unión con un mandato legal en el ámbito de la salud pública, los investigadores universitarios o las microempresas.

2. Las tasas a que se refiere el apartado 1 del presente artículo podrán incluir una compensación por los gastos soportados por el tenedor de datos de salud para recopilar y preparar los datos de salud electrónicos que vayan a ponerse a disposición para uso secundario. En dichos casos, el tenedor de datos de salud proporcionará una estimación de dichos costes al organismo de acceso a datos de salud. Cuando el tenedor de datos de salud sea un organismo del sector público, no se aplicará el artículo 6 del Reglamento (UE) 2022/868. La parte de las tasas vinculadas a los costes del tenedor de datos de salud se abonará al tenedor de datos de salud.

3. Las tasas cobradas a los usuarios de datos de salud en virtud del presente artículo serán transparentes y no discriminatorias.

4. Cuando los tenedores de datos de salud y los usuarios de datos de salud no lleguen a un acuerdo sobre el nivel de las tasas en el plazo de un mes a partir de la expedición del permiso de datos, el organismo de acceso a datos de salud podrá fijar las tasas en proporción al coste de la puesta a disposición de datos de salud electrónicos para uso secundario. Cuando el tenedor de datos de salud o el usuario de datos de salud no estén de acuerdo con la tasa fijada por el organismo de acceso a datos de salud, podrán recurrir a los órganos de resolución de litigios de conformidad con el artículo 10 del Reglamento (UE) 2023/2854.

5. Antes de expedir un permiso de datos con arreglo al artículo 68 o de responder a una petición de datos de salud presentada con arreglo al artículo 69, el organismo de acceso a datos de salud informará al solicitante de datos de salud sobre las tasas estimadas. Se informará al solicitante de datos de salud de la posibilidad de retirar la solicitud de acceso a datos de salud o la petición de datos de salud. En el caso de que el solicitante de datos de salud retire su solicitud o petición, únicamente se le cobrarán los gastos en que ya se haya incurrido.

6. La Comisión, mediante actos de ejecución, establecerá principios para las políticas y las estructuras de las tasas, incluidas las deducciones para las entidades a que se refiere el apartado 1, párrafo cuarto, del presente artículo a fin de respaldar la coherencia y transparencia entre los Estados miembros en relación con dichas políticas y estructuras de las tasas. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 63

Función de los organismos de acceso a datos de salud de garantizar el cumplimiento

1. En el ejercicio de sus funciones de seguimiento y supervisión a que se refiere el artículo 57, apartado 1, letra a), inciso ii), los organismos de acceso a datos de salud tendrán derecho a solicitar y recibir toda la información necesaria de los usuarios de datos de salud y de los tenedores de datos de salud para verificar el cumplimiento del presente capítulo.

2. Cuando los organismos de acceso a datos de salud constaten que un usuario de datos de salud o un tenedor de datos de salud no cumple los requisitos del presente capítulo, lo notificarán inmediatamente al usuario de datos de salud o al tenedor de datos de salud y adoptarán las medidas adecuadas. El organismo de acceso a datos de salud de que se trate dará al correspondiente usuario de datos de salud o tenedor de datos de salud la oportunidad de expresar su opinión en un plazo razonable, que no excederá de cuatro semanas.

Cuando la constatación de incumplimiento se refiera a una posible vulneración del Reglamento (UE) 2016/679, el organismo de acceso a datos de salud de que se trate informará inmediatamente a las autoridades de control con arreglo a dicho Reglamento y les proporcionará toda la información relevante relativa a dicha constatación.

3. Por lo que respecta al incumplimiento por parte de un usuario de datos de salud, los organismos de acceso a datos de salud estarán facultados para revocar el permiso de datos expedido con arreglo al artículo 68 y para detener sin demora indebida la operación de tratamiento de datos de salud electrónicos afectada que esté efectuando el usuario de datos de salud, y adoptarán medidas adecuadas y proporcionadas destinadas a garantizar el tratamiento conforme por parte del usuario de datos de salud.

Como parte de dichas medidas de garantía del cumplimiento, los organismos de acceso a datos de salud también podrán, cuando proceda, excluir o iniciar procedimientos para excluir al usuario de datos de salud en cuestión, de conformidad con el Derecho nacional, del acceso a datos de salud electrónicos del EEDS en el contexto de uso secundario durante un período de hasta cinco años.

4. Por lo que respecta al incumplimiento por parte de un tenedor de datos de salud, cuando un tenedor de datos de salud no ponga los datos de salud electrónicos a disposición de los organismos de acceso a datos de salud con la intención manifiesta de obstruir el uso de los datos de salud electrónicos, o no respete los plazos establecidos en el artículo 60, apartado 2, el organismo de acceso a datos de salud estará facultado para imponer al tenedor de datos de salud multas coercitivas por cada día de retraso, que deberán ser transparentes y proporcionadas. El organismo de acceso a datos de salud fijará el importe de las multas con arreglo al Derecho nacional. En caso de vulneraciones reiteradas por parte del tenedor de datos de salud de la obligación de cooperar con el organismo de acceso a datos de salud, dicho organismo podrá excluir, o iniciar procedimientos para excluir, al tenedor de datos de salud en cuestión, de conformidad con el Derecho nacional, de poder presentar solicitudes de acceso a datos de salud con arreglo al presente capítulo durante un período de hasta cinco años. Durante el período de exclusión, el tenedor de datos de salud seguirá estando obligado a proporcionar acceso a los datos en el marco del presente capítulo, cuando proceda.

5. El organismo de acceso a datos de salud comunicará sin demora al usuario de datos de salud o al tenedor de datos de salud afectados las medidas de garantía del cumplimiento adoptadas en virtud de los apartados 3 y 4, así como su justificación, y fijará un plazo razonable para que el usuario o tenedor de datos de salud cumpla las medidas.

6. Las medidas de garantía del cumplimiento adoptadas por el organismo de acceso a datos de salud en virtud del apartado 3 se notificarán a los demás organismos de acceso a datos de salud a través de la herramienta informática a que se refiere el apartado 7. Los organismos de acceso a datos de salud podrán poner a disposición del público esta información en sus sitios web.

7. La Comisión fijará, mediante actos de ejecución, la arquitectura de una herramienta informática, como parte integrante de la infraestructura de DatosSalud@UE a que se refiere el artículo 75, destinada a apoyar y hacer transparente para otros organismos de acceso a datos de salud las medidas de garantía del cumplimiento a que se refiere el presente artículo, especialmente las multas coercitivas, las revocaciones de permisos de datos y las exclusiones. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

8. A más tardar el 26 de marzo de 2032, la Comisión, en estrecha cooperación con el Consejo del EEDS, publicará directrices sobre las medidas de garantía del cumplimiento, incluidas las multas coercitivas y otras medidas, que deben adoptar los organismos de acceso a datos de salud.

Artículo 64

Condiciones generales para la imposición de multas administrativas por parte de los organismos de acceso a datos de salud

1. Cada organismo de acceso a datos de salud garantizará que la imposición de multas administrativas con arreglo al presente artículo por las infracciones a que se refieren los apartados 4 y 5 sean efectivas, proporcionadas y disuasorias en cada caso individual.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas de garantía del cumplimiento a que se refiere el artículo 63, apartados 3 y 4. Los organismos de acceso a datos de salud decidirán la imposición de una multa administrativa y su cuantía en cada caso individual teniendo en cuenta las circunstancias siguientes:

a) la naturaleza, la gravedad y la duración de la infracción;

b) si otras autoridades competentes ya han impuesto sanciones o multas administrativas por la misma infracción;

c) el carácter intencionado o negligente de la infracción;

d) cualquier medida adoptada por el tenedor de datos de salud o el usuario de datos de salud para atenuar los daños causados;

e) el grado de responsabilidad del usuario de datos de salud, teniendo en cuenta las medidas técnicas y organizativas que haya aplicado con arreglo al artículo 67, apartado 2, letra g), y al artículo 67, apartado 4;

f) cualquier infracción anterior pertinente por parte del tenedor de datos de salud o del usuario de datos de salud;

g) el grado de cooperación del tenedor de datos de salud o del usuario de datos de salud con el organismo de acceso a datos de salud en relación con poner remedio a la infracción y atenuar sus posibles efectos adversos;

h) la forma en que el organismo de acceso a datos de salud tuvo conocimiento de la infracción, en particular si el usuario de datos de salud notificó la infracción y, en tal caso, en qué medida;

i) el cumplimiento de cualquier medida de garantía del cumplimiento a que se refiere el artículo 63, apartados 3 y 4, que haya sido adoptada anteriormente contra el correspondiente responsable o encargado del tratamiento de los datos en relación con el mismo asunto;

j) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, mediante la infracción.

3. Si un tenedor de datos de salud o un usuario de datos de salud incumple de forma intencionada o negligente varias disposiciones del presente Reglamento respecto de los mismos permisos de datos o peticiones de datos de salud o de permisos o peticiones conexos, la cuantía total de la multa administrativa no será superior a la cuantía prevista para la infracción más grave.

4. De conformidad con el apartado 2 del presente artículo, las infracciones de las obligaciones del tenedor de datos de salud o del usuario de datos de salud contempladas en el artículo 60 y al artículo 61, apartados 1, 5 y 6, se sancionarán con multas administrativas de 10 000 000 EUR como máximo o, en el caso de una empresa, de una cuantía equivalente al 2 % como máximo de su volumen de negocios anual total a escala mundial del ejercicio financiero anterior si esta última cifra fuera superior.

5. De conformidad con el apartado 2, las infracciones siguientes se sancionarán con multas administrativas de 20 000 000 EUR como máximo o, en el caso de una empresa, de una cuantía equivalente al 4 % como máximo de su volumen de negocios anual total a escala mundial del ejercicio financiero anterior si esta última cifra fuera superior:

a) tratamiento para los usos contemplados en el artículo 54, por parte de un usuario de datos de salud, de datos de salud electrónicos obtenidos a través de un permiso de datos expedido con arreglo al artículo 68;

b) extracción de datos de salud electrónicos personales de entornos de tratamiento seguros por parte de un usuario de datos de salud;

c) reidentificación o intento de reidentificación de las personas físicas a las que se refieren los datos de salud electrónicos obtenidos por los usuarios de datos de salud sobre la base de un permiso de datos o una petición de datos de salud de conformidad con el artículo 61, apartado 3;

d) incumplimiento de las medidas de garantía del cumplimiento adoptadas por los organismos de acceso a datos de salud de conformidad con el artículo 63, apartados 3 y 4.

6. Sin perjuicio de las facultades de los organismos de acceso a datos de salud en virtud del artículo 63, cada Estado miembro podrá establecer reglas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos del sector público establecidos en dicho Estado miembro.

7. El ejercicio por un organismo de acceso a datos de salud de sus potestades en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y nacional, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

8. Cuando el ordenamiento jurídico de un Estado miembro no contemple multas administrativas, el presente artículo podrá aplicarse de tal modo que, de conformidad con su ordenamiento jurídico nacional, se garantice que las medidas jurídicas aplicadas sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por los organismos de acceso a datos de salud. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. El Estado miembro de que se trate notificará a la Comisión las disposiciones de la normativa que adopte en virtud del presente apartado a más tardar el 26 de marzo de 2029 y, sin demora, cualquier ley de modificación de dichas disposiciones o toda modificación posterior que las afecte.

Artículo 65

Relación con las autoridades de control del Reglamento (UE) 2016/679

La autoridad o las autoridades de control responsables de supervisar y garantizar la aplicación del Reglamento (UE) 2016/679 también serán competentes para supervisar y garantizar la aplicación del derecho de autoexclusión al tratamiento de los datos de salud electrónicos personales para uso secundario de conformidad con el artículo 71, y garantizar su cumplimiento. Las autoridades de control a que se refiere el párrafo primero del presente artículo estarán facultadas para imponer multas administrativas hasta el importe máximo a que se refiere el artículo 83 del Reglamento (UE) 2016/679.

Dichas autoridades de control y los organismos de acceso a datos de salud a que se refiere el artículo 55 del presente Reglamento cooperarán, cuando proceda, para garantizar el cumplimiento del presente Reglamento, en el marco de sus competencias respectivas. Se aplicarán *mutatis mutandis* las disposiciones pertinentes del Reglamento (UE) 2016/679.

SECCIÓN 3

Acceso a datos de salud electrónicos para uso secundario

Artículo 66

Minimización de datos y limitación de los fines

1. Cuando los organismos de acceso a datos de salud reciban una solicitud de acceso a datos de salud, garantizarán que solo se proporcione acceso a los datos de salud electrónicos que sean adecuados y pertinentes y se limiten a lo necesario en relación con los fines de tratamiento indicados en la solicitud de acceso a datos de salud por parte del usuario de datos de salud y en consonancia con el permiso de datos expedido con arreglo al artículo 68.

2. Los organismos de acceso a datos de salud proporcionarán los datos de salud electrónicos en un formato anonimizado, cuando los fines del tratamiento por el usuario de datos de salud puedan alcanzarse con dichos datos, teniendo en cuenta la información proporcionada por este.

3. Cuando el usuario de datos de salud haya demostrado suficientemente que los fines del tratamiento no pueden alcanzarse con datos anonimizados con arreglo al artículo 68, apartado 1, letra c), los organismos de acceso a datos de salud proporcionarán el acceso a datos de salud electrónicos en formato seudonimizado. La información necesaria para revertir la seudonimización solo estará a disposición del organismo de acceso a datos de salud o de una entidad que actúe como tercero fiable de conformidad con el Derecho nacional.

Artículo 67

Solicitudes de acceso a datos de salud

1. Cualquier persona física o jurídica podrá presentar una solicitud de acceso a datos de salud para los fines a que se refiere el artículo 53, apartado 1, a un organismo de acceso a datos de salud.

2. La solicitud de acceso a datos de salud incluirá:

a) la identidad del solicitante de datos de salud, una descripción de sus funciones y actividades profesionales, incluida la identidad de las personas físicas que vayan a tener acceso a los datos de salud electrónicos, en caso de que se expida un permiso de datos; el solicitante de datos de salud notificará al organismo de acceso a datos de salud toda actualización de la lista de personas físicas;

b) los fines a que se refiere el artículo 53, apartado 1, para los que se solicita el acceso;

c) una explicación pormenorizada del uso previsto de los datos de salud electrónicos y del beneficio previsto en relación con dicho uso y de la manera en que ese beneficio pueda contribuir a los fines a que se refiere el artículo 53, apartado 1;

d) una descripción de los datos de salud electrónicos solicitados, incluidos su alcance, período de tiempo, formato, fuentes y, cuando sea posible, la cobertura geográfica cuando se soliciten dichos datos de tenedores de datos de salud en varios Estados miembros o de participantes autorizados a los que se refiere el artículo 75;

e) una descripción explicativa de si los datos de salud electrónicos deben ponerse a disposición en un formato seudonimizado o anonimizado; en caso de un formato seudonimizado, una justificación de la razón por la que el tratamiento no puede realizarse mediante datos anonimizados;

f) cuando el solicitante de datos de salud tenga la intención de introducir en el entorno de tratamiento seguro conjuntos de datos que ya obren en su poder, una descripción de dichos conjuntos de datos;

g) una descripción de las garantías, que deben ser proporcionadas a los riesgos, previstas para prevenir cualquier uso indebido de los datos de salud electrónicos, así como para proteger los derechos e intereses del tenedor de datos de salud y de las personas físicas afectadas, también para evitar cualquier reidentificación de personas físicas en el conjunto de datos;

h) una indicación justificada del período necesario para el tratamiento de los datos de salud electrónicos en un entorno de tratamiento seguro;

i) una descripción de las herramientas y los recursos informáticos necesarios para un entorno de tratamiento seguro;

j) cuando proceda, información sobre toda evaluación de los aspectos éticos del tratamiento, exigida en virtud del Derecho nacional, que puede servir para sustituir la propia evaluación ética del solicitante de datos de salud;

k) cuando el solicitante de datos de salud tenga la intención de hacer uso de una excepción con arreglo al artículo 71, apartado 4, la justificación exigida por el Derecho nacional con arreglo a dicho artículo.

3. Cuando el solicitante de datos de salud desee acceder a datos de salud electrónicos que obren en poder de tenedores de datos de salud establecidos en más de un Estado miembro o de los participantes autorizados pertinentes en DatosSalud@UE a que se refiere el artículo 75, presentará una única solicitud de acceso a los datos de salud a través del organismo de acceso a datos de salud del Estado miembro donde esté situado el establecimiento principal del solicitante de datos de salud, a través del organismo de acceso a datos de salud del Estado miembro en el que esté establecido uno de esos tenedores de datos de salud o a través de los servicios prestados por la Comisión en DatosSalud@UE a que se refiere el artículo 75. La solicitud de acceso a datos de salud se transmitirá automáticamente a los participantes autorizados pertinentes en DatosSalud@UE y a los organismos de acceso a datos de salud de los Estados miembros en los que estén establecidos los tenedores de datos de salud identificados en la solicitud de acceso a datos de salud.

4. Cuando el solicitante de datos de salud desee acceder a los datos de salud electrónicos personales en un formato seudonimizado, proporcionará, junto con la solicitud de acceso a datos de salud, una descripción de la forma en que el tratamiento cumpliría lo dispuesto en el Derecho de la Unión y nacional aplicables en materia de protección de datos y privacidad, en particular el Reglamento (UE) 2016/679 y, más en concreto, su artículo 6, apartado 1.

5. Los organismos del sector público y las instituciones, órganos y organismos de la Unión proporcionarán la misma información que se exige en virtud de los apartados 2 y 4, excepto en el caso del apartado 2, letra h), en cuyo caso presentarán información sobre el período durante el cual se puede acceder a los datos de salud electrónicos, la frecuencia de dicho acceso o la frecuencia de las actualizaciones de los datos.

Artículo 68

Permiso de datos

1. A efectos de la concesión de acceso a los datos de salud electrónicos, los organismos de acceso a datos de salud evaluarán si se cumplen todos los criterios siguientes:

a) los fines descritos en la solicitud de acceso a datos de salud corresponden a uno o varios de los fines a que se refiere el artículo 53, apartado 1;

b) los datos solicitados son necesarios, adecuados y proporcionados para los fines descritos en la solicitud de acceso a datos de salud, teniendo en cuenta los requisitos de minimización de datos y limitación de los fines establecidos en el artículo 66;

c) el tratamiento cumple lo dispuesto en el artículo 6, apartado 1, del Reglamento (UE) 2016/679 y, en el caso de los datos seudonimizados, existe una justificación suficiente de que el fin no puede alcanzarse con datos anonimizados;

d) el solicitante de datos de salud está cualificado en relación con la finalidad prevista del uso de los datos y posee los conocimientos especializados adecuados, incluidas cualificaciones profesionales en los ámbitos de la asistencia sanitaria, la asistencia, la salud pública y la investigación, en consonancia con la práctica ética y las disposiciones legales y reglamentarias aplicables;

e) el solicitante de datos de salud demuestra suficientes medidas técnicas y organizativas para evitar cualquier uso indebido de los datos de salud electrónicos y para proteger los derechos y los intereses del tenedor de datos de salud y de las personas físicas de que se trate;

f) la información sobre la evaluación de los aspectos éticos del tratamiento, a que se refiere el artículo 67, apartado 2, letra j), cuando proceda, cumple con el Derecho nacional;

g) cuando el solicitante de datos de salud tenga intención de hacer uso de una excepción con arreglo al artículo 71, apartado 4, se ha proporcionado la justificación exigida por el Derecho nacional adoptado con arreglo a dicho artículo;

h) el solicitante de datos de salud cumple todos los demás requisitos del presente capítulo.

2. El organismo de acceso a datos de salud tendrá también en cuenta lo siguiente:

a) los riesgos para la defensa nacional, la seguridad, la seguridad pública y el orden público;

b) el riesgo de socavar la confidencialidad de los datos de las bases de datos de titularidad pública de las autoridades reguladoras.

3. Si el organismo de acceso a datos de salud llega a la conclusión de que se cumplen los requisitos del apartado 1 y de que los riesgos a que se refiere el apartado 2 se han atenuado suficientemente, el organismo de acceso a datos de salud concederá acceso a los datos de salud electrónicos mediante la expedición de un permiso de datos. Los organismos de acceso a datos de salud denegarán todas las solicitudes de acceso a datos de salud cuando no se cumplan los requisitos del presente capítulo.

Cuando no se cumplan los requisitos para la expedición de un permiso de datos, pero se cumplan los requisitos para proporcionar una respuesta en un formato estadístico anonimizado con arreglo al artículo 69, el organismo de acceso a datos de salud podrá decidir responder a condición de que tal respuesta atenúe los riesgos y, si el fin de la solicitud de acceso a datos de salud puede cumplirse de esta manera, de que el solicitante de datos de salud acepte recibir una respuesta en un formato estadístico anonimizado como dispone el artículo 69.

4. Como excepción a lo dispuesto en el Reglamento (UE) 2022/868, el organismo de acceso a datos de salud expedirá o denegará un permiso de datos en un plazo de tres meses a partir de la recepción de una solicitud de acceso a datos de salud completa. Si el organismo de acceso a datos de salud considera que la solicitud de acceso a datos de salud es incompleta, lo notificará al solicitante de datos de salud, que tendrá la posibilidad de completar dicha solicitud. Si el solicitante de datos de salud no completa la solicitud de acceso a datos de salud en un plazo de cuatro semanas, no se expedirá el permiso de datos.

El organismo de acceso a datos de salud podrá prorrogar hasta tres meses adicionales el plazo para responder a una solicitud de acceso a datos de salud cuando sea necesario, teniendo en cuenta la urgencia y la complejidad de la solicitud de acceso a datos de salud y el volumen de solicitudes de acceso a datos de salud presentadas. En tales casos, el organismo de acceso a datos de salud notificará lo antes posible al solicitante de datos de salud que se necesita más tiempo para examinar la solicitud de acceso a datos de salud, junto con los motivos de la demora.

5. Al tramitar una solicitud de acceso transfronterizo a datos de salud electrónicos a que se refiere el artículo 67, apartado 3, los organismos de acceso a datos de salud y los participantes autorizados pertinentes en DatosSalud@UE a que se refiere el artículo 75, seguirán siendo responsables de tomar las decisiones de concesión o denegación del acceso a los datos de salud electrónicos en el ámbito de sus competencias, de conformidad con el presente capítulo.

Los organismos de acceso a datos de salud y los participantes autorizados en DatosSalud@UE de que se trate se informarán mutuamente de sus decisiones. Podrán tener en cuenta esa información a la hora de decidir sobre la concesión o denegación del acceso a datos de salud electrónicos.

Un permiso de datos expedido por un organismo de acceso a datos de salud podrá beneficiarse del reconocimiento mutuo por parte de otro organismo de acceso a datos de salud.

6. Los Estados miembros establecerán un procedimiento acelerado de solicitud de acceso a datos de salud para los organismos del sector público y las instituciones, órganos y organismos de la Unión con un mandato legal en el ámbito de la salud pública si el tratamiento de los datos de salud electrónicos debe efectuarse para los fines establecidos en el artículo 53, apartado 1, letras a), b) y c).

Cuando se aplique dicho procedimiento acelerado, el organismo de acceso a datos de salud expedirá o denegará un permiso de datos en un plazo de dos meses a partir de la recepción de una solicitud de acceso a datos de salud completa. El organismo de acceso a datos de salud podrá prorrogar el plazo para responder a una solicitud de acceso a datos de salud en un mes adicional cuando sea necesario.

7. Tras la expedición del permiso de datos, el organismo de acceso a datos de salud solicitará inmediatamente al tenedor de datos de salud los datos de salud electrónicos. El organismo de acceso a datos de salud pondrá los datos de salud electrónicos a disposición del usuario de datos de salud en un plazo de dos meses a partir de que los haya recibido de los tenedores de datos de salud, a menos que el organismo de acceso a datos de salud especifique que los datos han de proporcionarse en un determinado plazo más largo.

8. En los casos a que se refiere el apartado 5, párrafo primero, del presente artículo, los organismos de acceso a datos de salud y los participantes autorizados en DatosSalud@UE que hayan expedido un permiso de datos o una aprobación de acceso, respectivamente, podrán decidir proporcionar acceso a los datos de salud electrónicos en el entorno de tratamiento seguro proporcionado por la Comisión a que se refiere el artículo 75, apartado 9.

9. Cuando el organismo de acceso a datos de salud deniegue la expedición del permiso de datos, deberá justificar esa denegación al solicitante de datos de salud.

10. Cuando expida un permiso de datos, el organismo de acceso a datos de salud establecerá en dicho permiso de datos las condiciones generales aplicables al usuario de datos de salud. El permiso de datos contendrá la información siguiente:

a) las categorías, la especificación y el formato de los datos de salud electrónicos a los que puede acceder, cubiertos por el permiso de datos, incluidas sus fuentes, y una indicación de si el acceso a los datos de salud electrónicos es en un formato seudonimizado en el entorno de tratamiento seguro;

b) una descripción pormenorizada de los fines para los que se ponen a disposición los datos de salud electrónicos;

c) cuando se prevea y sea aplicable algún mecanismo de excepción con arreglo al artículo 71, apartado 4, información sobre si se ha aplicado y el motivo de la correspondiente decisión;

d) la identidad de las personas autorizadas (en particular, la identidad del investigador principal) que tengan derecho a acceder a los datos de salud electrónicos en el entorno de tratamiento seguro;

e) la duración del permiso de datos;

f) información sobre las características técnicas y las herramientas de que dispone el usuario de datos de salud en el entorno de tratamiento seguro;

g) las tasas que deba pagar el usuario de datos de salud;

h) cualquier condición específica.

11. Los usuarios de datos de salud tendrán derecho a acceder a los datos de salud electrónicos y a tratarlos en un entorno de tratamiento seguro de conformidad con el permiso de datos que se les haya expedido en virtud del presente Reglamento.

12. El permiso de datos expedido tendrá la duración necesaria para cumplir los fines para los que se solicita, cuya duración no podrá exceder de diez años. Esta duración podrá prorrogarse una vez, por un período que no podrá exceder de diez años, a petición del usuario de datos de salud, sobre la base de argumentos y documentos que justifiquen dicha prórroga, presentados un mes antes de la expiración del permiso de datos. El organismo de acceso a datos de salud podrá aplicar tasas que vayan aumentando para reflejar los costes y riesgos del almacenamiento de datos de salud electrónicos durante un período superior al período inicial. Con el fin de reducir los costes y tasas, el organismo de acceso a datos de salud también podrá proponer al usuario de datos de salud que almacene el conjunto de datos en un sistema de almacenamiento con capacidades reducidas. Estas capacidades reducidas no deberán afectar a la seguridad del conjunto de datos tratado. Los datos de salud electrónicos en el entorno de tratamiento seguro se suprimirán en un plazo de seis meses a partir de la expiración del permiso de datos. A petición del usuario de datos de salud, el organismo de acceso a datos de salud podrá almacenar la fórmula utilizada para la creación del conjunto de datos solicitados.

13. Si es necesario actualizar el permiso de datos, el usuario de datos de salud deberá presentar una petición de modificación del permiso de datos.

14. La Comisión podrá desarrollar, mediante un acto de ejecución, un logotipo para hacer patente la contribución del EEDS. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 69

Petición de datos de salud

1. El solicitante de datos de salud podrá presentar una petición de datos de salud para los fines a que se refiere el artículo 53 con el fin de obtener una respuesta únicamente en formato estadístico anonimizado. Los organismos de acceso a datos de salud no responderán a una petición de datos en ningún otro formato y el usuario de datos de salud no tendrá acceso a los datos de salud electrónicos utilizados para proporcionar dicha respuesta.

2. Las peticiones de datos de salud a que se refiere el apartado 1 incluirán la información siguiente:

a) la identidad del solicitante de datos de salud y una descripción de las funciones profesionales y las actividades del solicitante de datos de salud;

b) una explicación pormenorizada del uso previsto de los datos de salud electrónicos, que incluya los fines a que se refiere el artículo 53, apartado 1, para los que se presenta la petición de datos de salud;

c) una descripción de los datos de salud electrónicos solicitados, su formato y las fuentes de dichos datos, cuando sea posible;

d) una descripción del contenido estadístico;

e) una descripción de las garantías previstas para evitar cualquier uso indebido de los datos de salud electrónicos solicitados;

f) una descripción de la forma en que el tratamiento cumpliría lo dispuesto en el artículo 6, apartado 1, del Reglamento (UE) 2016/679 o en el artículo 5, apartado 1, y el artículo 10, apartado 2, del Reglamento (UE) 2018/1725;

g) cuando el solicitante de datos de salud tenga intención de hacer uso de una excepción con arreglo al artículo 71, apartado 4, la justificación exigida a ese respecto por el Derecho nacional con arreglo a dicho artículo.

3. El organismo de acceso a datos de salud evaluará si la petición de datos de salud está completa y tendrá en cuenta los riesgos a que se refiere el artículo 68, apartado 2.

4. El organismo de acceso a datos de salud evaluará la petición de datos de salud en un plazo de tres meses desde la recepción de la petición, y, cuando sea posible, proporcionará posteriormente la respuesta al usuario de datos de salud en un plazo adicional de tres meses.

Artículo 70

Modelos para apoyar el acceso a datos de salud electrónicos para uso secundario

A más tardar el 26 de marzo de 2027, la Comisión establecerá, mediante actos de ejecución, los modelos para la solicitud de acceso a datos de salud, los permisos de datos y las peticiones de datos de salud a que se refieren los artículos 67, 68 y 69, respectivamente. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 71

Derecho de autoexclusión del tratamiento de datos de salud electrónicos personales para uso secundario

1. Las personas físicas tendrán derecho de autoexclusión, en cualquier momento y sin necesidad de exponer los motivos, del tratamiento de los datos de salud electrónicos personales que les conciernan para uso secundario en el marco del presente Reglamento. El ejercicio de ese derecho será revocable.

2. Los Estados miembros proporcionarán un mecanismo de autoexclusión accesible y de fácil comprensión para el ejercicio del derecho establecido en el apartado 1, con arreglo al cual las personas físicas podrán manifestar expresamente que no desean que sus datos de salud electrónicos personales sean tratados para uso secundario.

3. Una vez que las personas físicas hayan ejercido el derecho de autoexclusión, y cuando los datos de salud electrónicos personales que les conciernan puedan identificarse en un conjunto de datos, los datos de salud electrónicos personales que conciernan a esas personas físicas no se pondrán a disposición ni se tratarán de otro modo con arreglo a permisos de datos expedidos de conformidad con el artículo 68 o a peticiones de datos de salud con arreglo al artículo 69 aprobadas después de que la persona física haya ejercido su derecho de autoexclusión.

El párrafo primero no afectará al tratamiento para uso secundario de los datos de salud electrónicos personales relativos a dichas personas físicas con arreglo a permisos de datos expedidos o solicitudes de datos de salud aprobadas antes de que las personas físicas hayan ejercido su derecho de autoexclusión.

4. Como excepción al derecho de autoexclusión dispuesto en el apartado 1, los Estados miembros podrán prever en su Derecho nacional un mecanismo para poner a disposición datos respecto de los cuales se haya ejercido el derecho de autoexclusión, siempre y cuando se cumplan todas las condiciones siguientes:

a) la solicitud de acceso a datos de salud o la petición de datos de salud sea presentada por un organismo del sector público o una institución, órgano u organismo de la Unión con mandato para desempeñar una misión en el ámbito de la salud pública, o por otra entidad a la que se haya encomendado la realización de una misión pública en el ámbito de la salud pública, o que actúe en nombre o por encargo de una autoridad pública, y el tratamiento de dichos datos sea necesario para cualquiera de los fines siguientes:

i) los fines a que se refiere el artículo 53, apartado 1, letras a), b) y c),

ii) investigación científica por razones importantes de interés público;

b) dichos datos no puedan obtenerse por medios alternativos de manera oportuna y eficaz en condiciones equivalentes;

c) el solicitante de datos de salud haya presentado la justificación a que se refiere el artículo 68, apartado 1, letra g), o el artículo 69, apartado 2, letra g).

El Derecho nacional que establezca dicho mecanismo dispondrá medidas específicas y adecuadas a fin de proteger los derechos fundamentales y los datos personales de las personas físicas.

Cuando un Estado miembro haya previsto en su Derecho nacional la posibilidad de pedir acceso a los datos respecto de los cuales se haya ejercido el derecho de autoexclusión y se cumplan las condiciones a que se refiere el párrafo primero del presente apartado, dichos datos podrán incluirse al desempeñar las funciones previstas en el artículo 57, apartado 1, letra a), incisos i) y iii), y letra b).

5. Las disposiciones sobre cualquier mecanismo de excepción establecido en virtud del apartado 4 como excepción al apartado 1, deberá respetar en lo esencial los derechos y libertades fundamentales y serán una medida necesaria y proporcionada en una sociedad democrática para satisfacer los fines de interés público en el ámbito de los objetivos científicos y sociales legítimos.

6. Todo tratamiento efectuado con arreglo a algún mecanismo de excepción establecido en virtud del apartado 4 del presente artículo deberá cumplir los requisitos del presente capítulo, en particular la prohibición de reidentificación o de intentar reidentificar a personas físicas de conformidad con el artículo 61, apartado 3. Toda medida legislativa que prevea un mecanismo en Derecho nacional tal como dispone el apartado 4 del presente artículo incluirá disposiciones específicas para la seguridad de las personas físicas y la protección de sus derechos.

7. Los Estados miembros notificarán sin demora a la Comisión las disposiciones de Derecho nacional que adopten de conformidad con el apartado 4 así como toda modificación posterior.

8. Cuando los fines de tratamiento de datos de salud electrónicos personales por un tenedor de datos de salud no requieren o ya no requieren la identificación de un interesado por parte del responsable del tratamiento, dicho tenedor de datos de salud no estará obligado a mantener, adquirir o tratar información adicional para identificar al interesado con el único fin de cumplir el derecho de autoexclusión en virtud del presente artículo.

Artículo 72

Procedimiento simplificado para el acceso a los datos de salud electrónicos de un tenedor fiable de datos de salud

1. Cuando un organismo de acceso a datos de salud reciba una solicitud de acceso a datos de salud con arreglo al artículo 67 o una petición de datos de salud con arreglo al artículo 69, que solo abarque los datos de salud electrónicos en poder de un tenedor fiable de datos de salud designado con arreglo al apartado 2 del presente artículo, se aplicará el procedimiento determinado en los apartados 4 a 6 del presente artículo.

2. Los Estados miembros podrán establecer un procedimiento por el que los tenedores de datos de salud puedan solicitar ser designados como tenedores fiables de datos de salud, siempre que los tenedores de datos de salud cumplan las condiciones siguientes:

a) pueden proporcionar acceso a los datos de salud a través de un entorno de tratamiento seguro que cumpla lo dispuesto en el artículo 73;

b) cuentan con los conocimientos especializados necesarios para evaluar las solicitudes de acceso a datos de salud y las peticiones de datos de salud;

c) ofrecen las garantías necesarias para garantizar el cumplimiento del presente Reglamento.

Los Estados miembros designarán tenedores fiables de datos de salud tras una evaluación del cumplimiento de esas condiciones por parte del organismo de acceso a datos de salud pertinente.

Los Estados miembros establecerán un procedimiento para revisar periódicamente si el tenedor fiable de datos de salud sigue cumpliendo esas condiciones.

Los organismos de acceso a datos de salud indicarán los tenedores fiables de datos de salud en el catálogo de conjuntos de datos a que se refiere el artículo 77.

3. Las solicitudes de acceso a datos de salud y las peticiones de datos de salud a que se refiere el apartado 1 se presentarán al organismo de acceso a datos de salud, que podrá transmitirlas al tenedor fiable de datos de salud pertinente.

4. Tras la recepción de la solicitud de acceso a datos de salud o de la petición de datos de salud con arreglo al apartado 3 del presente artículo, el tenedor fiable de datos de salud evaluará la solicitud de acceso a datos de salud o la petición de datos de salud contrastándola con los criterios enumerados en el artículo 68, apartados 1 y 2, o en el artículo 69, apartados 2 y 3, según proceda.

5. El tenedor fiable de datos de salud presentará la evaluación efectuada de conformidad con el apartado 4, acompañada de una propuesta de decisión, al organismo de acceso a datos de salud en un plazo de dos meses a partir de la recepción de la solicitud de datos de salud o petición de datos de salud de dicho organismo. En un plazo de dos meses a partir de la recepción de la evaluación, el organismo de acceso a datos de salud emitirá una decisión sobre la solicitud de acceso a datos de salud o la petición de datos de salud. El organismo de acceso a datos de salud no estará vinculado por la propuesta presentada por el tenedor fiable de datos de salud.

6. Tras la decisión del organismo de acceso a datos de salud de expedir el permiso de datos o de aprobar la petición de datos de salud, el tenedor fiable de datos de salud desempeñará las funciones a que se refieren el artículo 57, apartado 1, letra a), inciso i), y letra b).

7. El servicio de acceso a datos de salud de la Unión a que se refiere el artículo 56 podrá designar tenedores de datos de salud que sean instituciones, órganos u organismos de la Unión que cumplan las condiciones establecidas en el apartado 2, párrafo primero, letras a), b) y c), como tenedores fiables de datos de salud. Cuando lo haga, se aplicarán *mutatis mutandis* el apartado 2, párrafos tercero y cuarto, y los apartados 3 a 6 del presente artículo.

Artículo 73

Entorno de tratamiento seguro

1. Los organismos de acceso a datos de salud proporcionarán acceso a los datos de salud electrónicos en virtud de un permiso de datos únicamente a través de un entorno de tratamiento seguro sometido a medidas técnicas y organizativas y requisitos de seguridad e interoperabilidad. En particular, el entorno de tratamiento seguro deberá cumplir las medidas de seguridad siguientes:

a) limitar el acceso al entorno de tratamiento seguro a las personas físicas autorizadas enumeradas en el permiso de datos expedido con arreglo al artículo 68;

b) minimizar el riesgo de lectura, copia, modificación o supresión no autorizadas de los datos de salud electrónicos alojados en un entorno de tratamiento seguro a través de las medidas técnicas y organizativas más avanzadas;

c) limitar la introducción de datos de salud electrónicos y la inspección, modificación o supresión de los datos de salud electrónicos alojados en el entorno de tratamiento seguro a un número limitado de personas identificables autorizadas;

d) garantizar que los usuarios de datos de salud solo tengan acceso a los datos de salud electrónicos cubiertos por su permiso de datos, únicamente mediante identidades de usuario individuales y únicas y modos de acceso confidenciales;

e) conservar registros identificables de acceso al entorno de tratamiento seguro y de las actividades en él durante el período necesario para verificar y auditar todas las operaciones de tratamiento en dicho entorno; los registros de acceso se conservarán durante un período de al menos un año;

f) garantizar el cumplimiento y realizar un seguimiento de las medidas de seguridad a que se refiere el presente apartado para atenuar las posibles amenazas para la seguridad.

2. Los organismos de acceso a datos de salud garantizarán que los tenedores de datos de salud puedan cargar los datos de salud electrónicos en el formato que especifique el permiso de datos y que el usuario de datos de salud pueda acceder a ellos en un entorno de tratamiento seguro.

Los organismos de acceso a datos de salud revisarán los datos de salud electrónicos incluidos en una petición de descarga con objeto de garantizar que los usuarios de datos de salud solo puedan descargar datos de salud electrónicos no personales, incluidos los datos de salud electrónicos en un formato estadístico anonimizado, desde el entorno de tratamiento seguro.

3. Los organismos de acceso a datos de salud se asegurarán de que se realicen auditorías periódicas de los entornos de tratamiento seguros, también por terceros, y adoptarán medidas correctivas con respecto a cualquier deficiencia, riesgo o vulnerabilidad detectados por dichas auditorías en los entornos de tratamiento seguros.

4. Cuando las organizaciones de cesión altruista de datos reconocidas contempladas en el capítulo IV del Reglamento (UE) 2022/868 traten datos de salud electrónicos personales utilizando un entorno de tratamiento seguro, dichos entornos también deberán cumplir las medidas de seguridad establecidas en el apartado 1, letras a) a f), del presente artículo.

5. A más tardar el 26 de marzo de 2027, la Comisión establecerá, mediante actos de ejecución, los requisitos técnicos, organizativos, de seguridad de la información, de confidencialidad, de protección de datos y de interoperabilidad para los entornos de tratamiento seguros, también con respecto a las características técnicas y las herramientas a disposición del usuario de datos de salud en el entorno de tratamiento seguro. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 74

Responsabilidad del tratamiento

1. El tenedor de los datos de salud se considerará responsable del tratamiento respecto del acto de poner los datos de salud electrónicos personales a disposición del organismo de acceso a datos de salud, solicitado de conformidad con el artículo 60, apartado 1.

El organismo de acceso a datos de salud se considerará responsable del tratamiento de los datos de salud electrónicos personales cuando desempeñe sus funciones con arreglo al presente Reglamento.

No obstante lo dispuesto en el párrafo segundo del presente apartado, se considerará que el organismo de acceso a datos de salud actúa como encargado del tratamiento en nombre del usuario de datos de salud como responsable del tratamiento de datos de salud electrónicos personales con arreglo a un permiso de datos expedido con arreglo al artículo 68 en el entorno de tratamiento seguro cuando proporcione datos a través de dicho entorno o por el tratamiento de dichos datos con arreglo a una petición de datos de salud aprobada en virtud del artículo 69 para generar una respuesta.

2. En las situaciones a que se refiere el artículo 72, apartado 6, el tenedor fiable de datos de salud se considerará responsable del tratamiento de datos de salud electrónicos personales en relación con el suministro de datos de salud electrónicos al usuario de datos de salud con arreglo a un permiso de datos o a una petición de datos de salud. Se considerará que el tenedor de datos de salud fiable actúa como encargado del tratamiento en nombre del usuario de datos de salud cuando proporcione datos a través de un entorno de tratamiento seguro.

3. La Comisión podrá establecer, mediante actos de ejecución, un modelo para los acuerdos entre responsables del tratamiento y encargados del tratamiento en el marco de los apartados 1 y 2 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

SECCIÓN 4

Infraestructura transfronteriza para el uso secundario

Artículo 75

DatosSalud@UE

1. Cada Estado miembro designará un punto de contacto nacional para uso secundario. Ese punto de contacto nacional para uso secundario será una pasarela organizativa y técnica que permita y sea responsable de poner a disposición los datos de salud electrónicos para uso secundario en un contexto transfronterizo. El punto de contacto nacional para uso secundario podrá ser el coordinador del organismo de acceso a datos de salud a que se refiere el artículo 55, apartado 1. Cada Estado miembro informará a la Comisión del nombre y los datos de contacto del punto de contacto nacional para uso secundario a más tardar el 26 de marzo de 2027. La Comisión y los Estados miembros pondrán dicha información a disposición del público.

2. El servicio de acceso a datos de salud de la Unión actuará como punto de contacto de las instituciones, órganos y organismos de la Unión para uso secundario y será responsable de poner los datos de salud electrónicos a disposición para uso secundario.

3. Los puntos de contacto nacionales para uso secundario a que se refiere el apartado 1 y el servicio de acceso a datos de salud de la Unión a que se refiere el apartado 2 estarán conectados a la infraestructura transfronteriza para el uso secundario, a saber, DatosSalud@UE. Los puntos de contacto nacionales de uso secundario y el servicio de acceso a datos de salud de la Unión facilitarán el acceso transfronterizo a los datos de salud electrónicos para uso secundario a los diferentes participantes autorizados en DatosSalud@UE. Los puntos de contacto nacionales para uso secundario cooperarán estrechamente entre sí y con la Comisión.

4. Las infraestructuras de investigación relacionadas con la salud o las infraestructuras similares cuyo funcionamiento se base en el Derecho de la Unión y que presten apoyo para el uso de datos de salud electrónicos con fines de investigación, formulación de políticas, estadísticas, seguridad de los pacientes o de regulación podrán ser participantes autorizados en DatosSalud@UE y estar conectados a ella.

5. Los terceros países o las organizaciones internacionales podrán ser participantes autorizados en DatosSalud@UE cuando cumplan las disposiciones del presente capítulo y proporcionen a los usuarios de datos de salud situados en la Unión, en términos y condiciones equivalentes, acceso a los datos de salud electrónicos de que dispongan sus organismos de acceso a datos de salud, siempre que cumplan lo dispuesto en el capítulo V del Reglamento (UE) 2016/679.

La Comisión podrá determinar, mediante actos de ejecución, el cumplimiento de un punto de contacto nacional para uso secundario de un tercer país o de un sistema establecido a nivel internacional por organizaciones internacionales con los requisitos de DatosSalud@UE a efectos del uso secundario de datos de salud y con el presente capítulo y que da acceso a los usuarios de datos de salud situados en la Unión a los datos de salud electrónicos a los que tiene acceso en condiciones equivalentes a las de DatosSalud@UE. El cumplimiento de esos requisitos jurídicos, organizativos, técnicos y de seguridad, incluidos los requisitos para entornos de tratamiento seguros previstos en el artículo 73, se comprobará bajo el control de la Comisión. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2. La Comisión hará pública la lista de actos de ejecución adoptados en virtud del presente apartado.

6. Se dotará a cada punto de contacto nacional para uso secundario y a cada participante autorizado en DatosSalud@UE de la capacidad técnica necesaria para conectarse y participar en DatosSalud@UE. Dichos puntos y participantes cumplirán los requisitos y especificaciones técnicas necesarios para explotar DatosSalud@UE y permitirles conectarse a ella.

7. Los Estados miembros y la Comisión crearán la infraestructura DatosSalud@UE para apoyar y facilitar el acceso transfronterizo a los datos de salud electrónicos para uso secundario, conectando los puntos de contacto nacionales para uso secundario y los participantes autorizados en DatosSalud@UE y la plataforma central a que se refiere el apartado 8.

8. La Comisión desarrollará, implantará y explotará una plataforma central para DatosSalud@UE, proporcionando los servicios de tecnología de la información necesarios para apoyar y facilitar el intercambio de información entre los organismos de acceso a datos de salud como parte de DatosSalud@UE. La Comisión solo tratará los datos de salud electrónicos en nombre de los responsables del tratamiento como encargada del tratamiento.

9. Cuando lo soliciten dos o más puntos de contacto nacionales para uso secundario, la Comisión podrá proporcionar un entorno de tratamiento seguro que cumplan los requisitos del artículo 73 para los datos procedentes de más de un Estado miembro. Cuando dos o más puntos de contacto nacionales para uso secundario o participantes autorizados en DatosSalud@UE introduzcan datos de salud electrónicos en el entorno de tratamiento seguro gestionado por la Comisión, serán corresponsables del tratamiento y la Comisión será la encargada del tratamiento a efectos del tratamiento de datos en ese entorno.

10. Los puntos de contacto nacionales para uso secundario actuarán como corresponsables de las operaciones de tratamiento realizadas en DatosSalud@UE en las que participen y la Comisión actuará como encargada del tratamiento en nombre de dichos puntos de contacto nacionales para uso secundario, sin afectar a las funciones de los organismos de acceso a datos de salud antes y después de estas operaciones de tratamiento.

11. Los Estados miembros y la Comisión procurarán garantizar que DatosSalud@UE sea interoperable con otros espacios comunes europeos de datos pertinentes a que se refieren los Reglamentos (UE) 2022/868 y (UE) 2023/2854.

12. A más tardar el 26 de marzo de 2027, la Comisión establecerá, mediante actos de ejecución:

a) los requisitos, las especificaciones técnicas y la arquitectura informática de DatosSalud@UE, que garantizarán un avanzado nivel de seguridad de los datos, confidencialidad y protección de los datos de salud electrónicos en DatosSalud@UE;

b) las condiciones y comprobaciones del cumplimiento que se requieran para poder unirse y permanecer conectado a DatosSalud@UE, así como las condiciones de desconexión temporal o exclusión definitiva de esta, incluidas las disposiciones específicas en caso de falta grave o infracción reiterada;

c) los criterios mínimos que deben cumplir los puntos de contacto nacionales para uso secundario y los participantes autorizados en DatosSalud@UE;

d) las responsabilidades de los responsables y de los encargados del tratamiento que participen en DatosSalud@UE;

e) las responsabilidades de los responsables y de los encargados del tratamiento en relación con el entorno de tratamiento seguro gestionado por la Comisión;

f) especificaciones comunes para la arquitectura de DatosSalud@UE y para su interoperabilidad con otros espacios comunes europeos de datos.

Los actos de ejecución a que se refiere el párrafo primero del presente apartado se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

13. Cuando haya un resultado positivo de la comprobación del cumplimiento a que se refiere el apartado 5 del presente artículo, la Comisión podrá adoptar, mediante actos de ejecución, las decisiones de conectar a participantes autorizados concretos en DatosSalud@UE. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 76

Acceso a registros o bases de datos transfronterizos de datos de salud electrónicos para uso secundario

1. En el caso de los registros y las bases de datos transfronterizos, el organismo de acceso a datos de salud en el que esté registrado el tenedor de datos de salud para el registro o la base de datos específicos será competente para decidir sobre las solicitudes de acceso a datos de salud para poder acceder a los datos de salud electrónicos con arreglo a un permiso de datos. Cuando dichos registros o bases de datos tengan corresponsables del tratamiento, el organismo de acceso a datos de salud que decida sobre las solicitudes de acceso a datos de salud que deban utilizarse para proporcionar acceso a datos de salud electrónicos será el organismo de acceso a datos de salud del Estado miembro en el que esté establecido uno de los corresponsables del tratamiento.

2. Cuando los registros o las bases de datos de varios Estados miembros se organicen en una única red de registros o bases de datos a escala de la Unión, los registros o bases de datos asociados podrán designar un coordinador para garantizar el suministro de datos de la red de registros o bases de datos para uso secundario. El organismo de acceso a datos de salud del Estado miembro en el que esté establecido el coordinador de la red será competente para decidir sobre las solicitudes de acceso a datos de salud que deban utilizarse para proporcionar acceso a los datos de salud electrónicos de la red de registros o de bases de datos.

SECCIÓN 5

Calidad y utilidad de los datos de salud para uso secundario

Artículo 77

Descripción de un conjunto de datos y catálogo de conjuntos de datos

1. Los organismos de acceso a datos de salud, a través de un catálogo de conjuntos de datos normalizado y accesible al público y legible por máquina, proporcionarán una descripción en forma de metadatos de los conjuntos de datos disponibles y sus características. La descripción de cada conjunto de datos incluirá información sobre la fuente, el alcance, las principales características y la naturaleza de los datos de salud electrónicos en el conjunto de datos y las condiciones de disponibilidad de dichos datos.

2. Las descripciones de los conjuntos de datos del catálogo nacional de conjuntos de datos estarán disponibles, como mínimo, en una lengua oficial de la Unión. El catálogo de conjuntos de datos para las instituciones, órganos y organismos de la Unión proporcionado por el servicio de acceso a datos de salud de la Unión estará disponible en todas las lenguas oficiales de la Unión.

3. El catálogo de conjuntos de datos se pondrá a disposición de los puntos únicos de información establecidos o designados con arreglo al artículo 8 del Reglamento (UE) 2022/868.

4. A más tardar el 26 de marzo de 2027, la Comisión establecerá, mediante actos de ejecución, los elementos mínimos que deben proporcionar los tenedores de datos de salud para los conjuntos de datos y las características de esos elementos. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 78

Etiqueta de calidad y utilidad de los datos

1. Los conjuntos de datos disponibles a través de los organismos de acceso a datos de salud podrán obtener de los tenedores de datos de salud una etiqueta de la Unión relativa a la calidad y utilidad de los datos.

2. Los conjuntos de datos que contengan datos de salud electrónicos recogidos y tratados con el apoyo de la financiación pública nacional o de la Unión tendrán una etiqueta de calidad y utilidad de los datos que cubra los elementos indicados en el apartado 3.

3. La etiqueta de calidad y utilidad de los datos cubrirá los elementos siguientes, si procede:

a) para la documentación de datos: los metadatos, la documentación de apoyo, el diccionario de datos, el formato y normas utilizadas, la fuente de los datos y, en su caso, el modelo de datos;

b) para la evaluación de la calidad técnica: la exhaustividad, la singularidad, la exactitud, la validez, la oportunidad y la coherencia de los datos;

c) para los procesos de gestión de la calidad de los datos: el nivel de madurez de los procesos de gestión de la calidad de los datos, incluidos los procesos de revisión y auditoría y el examen de sesgos;

d) para la evaluación de la cobertura: el período de tiempo, la cobertura de población y, en su caso, la representatividad de la población incluida en la muestra y el marco temporal medio en el que una persona física aparece en un conjunto de datos;

e) para la información sobre el acceso y el suministro: el tiempo transcurrido entre la recogida de los datos de salud electrónicos y su inclusión en el conjunto de datos, y el plazo para el suministro de los datos de salud electrónicos tras la expedición de un permiso de datos o la aprobación de una solicitud de acceso a estos;

f) para la información sobre las modificaciones de datos: la combinación e incorporación de datos en un conjunto de datos existente, incluidos los enlaces con otros conjuntos de datos.

4. Cuando un organismo de acceso a datos de salud tenga motivos para creer que una etiqueta de calidad y utilidad de los datos pueda ser inexacta, evaluará si el conjunto de datos cubierto por la etiqueta cumple los requisitos de calidad que forman parte de los elementos de la etiqueta de calidad y utilidad de los datos a que se refiere el apartado 3 y, en caso de que el conjunto de datos no cumple los requisitos de calidad, revocará la etiqueta.

5. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 97 en lo referente a la modificación del presente Reglamento para modificar, añadir o suprimir elementos que la etiqueta de calidad y utilidad de los datos establecida en el apartado 3 del presente artículo deba cubrir.

6. A más tardar el 26 de marzo de 2027, la Comisión establecerá, mediante actos de ejecución, las características visuales y las especificaciones técnicas de la etiqueta de calidad y utilidad de los datos, sobre la base de los elementos a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2, del presente Reglamento. Dichos actos de ejecución tendrán en cuenta los requisitos del artículo 10 del Reglamento (UE) 2024/1689 y, en su caso, cualquier especificación común o norma armonizada adoptada que incorpore dichos requisitos.

Artículo 79

Catálogo de conjuntos de datos de la UE

1. La Comisión establecerá un catálogo de conjuntos de datos de la UE que conecte los catálogos de conjuntos de datos nacionales establecidos por los organismos de acceso a datos de salud en cada Estado miembro y los catálogos de conjuntos de datos de los participantes autorizados en DatosSalud@UE.

2. El catálogo de conjuntos de datos de la UE, los catálogos de conjuntos de datos nacionales y los catálogos de conjuntos de datos de los participantes autorizados en DatosSalud@UE se pondrán a disposición del público.

Artículo 80

Especificaciones mínimas para conjuntos de datos de alto impacto

La Comisión podrá determinar, mediante actos de ejecución, las especificaciones mínimas de los conjuntos de datos de alto impacto para uso secundario, teniendo en cuenta las infraestructuras, normas, directrices y recomendaciones de la Unión existentes. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

SECCIÓN 6

Reclamaciones

Artículo 81

Derecho a reclamar ante organismos de acceso a datos de salud

1. Sin perjuicio de cualquier otro recurso administrativo o judicial, las personas físicas o jurídicas tendrán derecho a reclamar en relación con lo dispuesto en el presente capítulo, ya sea de forma individual o, en su caso, colectiva, ante un organismo de acceso a datos de salud, siempre que los derechos o intereses de dichas personas se vean afectados negativamente.

2. El organismo de acceso a datos de salud ante el que se haya presentado la reclamación informará al reclamante sobre el estado en que se encuentre la tramitación de la reclamación y sobre la decisión que se tome acerca de la reclamación.

3. Los organismos de acceso a datos de salud proporcionarán herramientas de fácil acceso para la presentación de reclamaciones.

4. Cuando la reclamación se refiera a los derechos de las personas físicas en virtud del artículo 71 del presente Reglamento, dicha reclamación se transmitirá a la autoridad de control competente de conformidad con el Reglamento (UE) 2016/679. El organismo de acceso a datos de salud pertinente proporcionará a dicha autoridad de control la información necesaria a su disposición de conformidad con el Reglamento (UE) 2016/679 a fin de facilitar la evaluación y la investigación de la reclamación.

CAPÍTULO V

MEDIDAS ADICIONALES

Artículo 82

Desarrollo de capacidades

La Comisión apoyará el intercambio de mejores prácticas y conocimientos especializados para desarrollar las capacidades en los Estados miembros de reforzar los sistemas de salud digital para uso primario y secundario teniendo en cuenta las circunstancias específicas de las diferentes categorías de partes interesadas implicadas. Para apoyar ese desarrollo de capacidades, la Comisión, en estrecha cooperación y consulta con los Estados miembros, establecerá indicadores de autoevaluación para uso primario y secundario.

Artículo 83

Programas de formación e información para los profesionales sanitarios

1. Los Estados miembros desarrollarán y aplicarán programas de formación o proporcionarán acceso a ellos y proporcionarán acceso a la información para los profesionales sanitarios con el fin de que comprendan y desempeñen eficazmente sus funciones en el uso primario de los datos de salud electrónicos y en el acceso a ellos, también en relación con los artículos 11, 13 y 16. La Comisión apoyará a los Estados miembros a este respecto.

2. Los programas de formación y la información serán accesibles y asequibles para todos los profesionales sanitarios, sin perjuicio de la organización de los sistemas de asistencia sanitaria a nivel nacional.

Artículo 84

Alfabetización en materia de salud digital y acceso a la salud digital

1. Los Estados miembros promoverán y apoyarán la alfabetización en materia de salud digital y el desarrollo de las competencias y capacidades pertinentes para los pacientes. La Comisión apoyará a los Estados miembros a este respecto. Las campañas o programas de sensibilización tendrán por objeto, en particular, informar a los pacientes y al público en general sobre uso primario y secundario en el marco del EEDS, incluidos los derechos que se derivan de él, así como las ventajas, los riesgos y los posibles beneficios del uso primario y secundario para la ciencia y la sociedad.

2. Las campañas y programas de sensibilización a que se refiere el apartado 1 se adaptarán a las necesidades de grupos específicos y se desarrollarán, revisarán y, en caso necesario, se actualizarán.

3. Los Estados miembros promoverán el acceso a la infraestructura necesaria para la gestión eficaz de los datos de salud electrónicos de las personas físicas, tanto para uso primario como secundario.

Artículo 85

Requisitos adicionales para la contratación pública y la financiación de la Unión

1. Los poderes adjudicadores, incluidas las autoridades de salud digital, los organismos de acceso a datos de salud y las instituciones, órganos u organismos de la Unión, harán referencia a las especificaciones técnicas, normas y perfiles aplicables a que se refieren los artículos 15, 23, 36, 73, 75 y 78, para los procedimientos de contratación pública y cuando redacten sus documentos de licitación o convocatorias de propuestas, así como para definir las condiciones de financiación de la Unión en relación con el presente Reglamento, incluidas las condiciones favorables para los Fondos Estructurales y de cohesión.

2. Los criterios para la obtención de financiación de la Unión tendrán en cuenta los requisitos desarrollados en el marco de los capítulos II, III y IV.

Artículo 86

Almacenamiento de datos de salud electrónicos personales para uso primario

De conformidad con los principios generales del Derecho de la Unión, que incluyen los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, los Estados miembros garantizarán que exista un nivel especialmente elevado de protección y seguridad en el tratamiento de los datos de salud electrónicos personales para uso primario, mediante medidas técnicas y organizativas adecuadas. A este respecto, el presente Reglamento no es obstáculo para un requisito establecido en el Derecho nacional que tenga en cuenta el contexto nacional, según el cual, cuando los datos de salud electrónicos personales sean tratados por prestadores de asistencia sanitaria para la prestación de asistencia sanitaria o por los puntos de contacto nacionales para la salud digital conectados a MiSalud@UE, el almacenamiento de los datos de salud electrónicos personales a que se refiere el artículo 14 del presente Reglamento con fines de uso primario se sitúe en la Unión, de conformidad con el Derecho de la Unión y los compromisos internacionales.

Artículo 87

Almacenamiento de datos de salud electrónicos personales por organismos de acceso a datos de salud y entornos de tratamiento seguros

1. Los organismos de acceso a datos de salud, los tenedores de datos de salud fiables y el servicio de acceso a datos de salud de la Unión almacenarán y tratarán datos de salud electrónicos personales en la Unión cuando realicen seudonimización, anonimización y cualquier otra operación de tratamiento de datos personales a que se refieren los artículos 67 a 72, a través de entornos de tratamiento seguros en el sentido del artículo 73 y del artículo 75, apartado 9, o a través de DatosSalud@UE. Este requisito se aplicará a cualquier entidad que realice esas funciones en nombre de dichos organismos, tenedores o servicios.

2. Como excepción a lo dispuesto en el apartado 1 del presente artículo, los datos a que se refiere dicho apartado podrán almacenarse y tratarse en un tercer país, o un territorio o uno o varios sectores específicos dentro de ese tercer país, cuando a dicho país, territorio o sector se aplique una decisión de adecuación adoptada en virtud del artículo 45 del Reglamento (UE) 2016/679.

Artículo 88

Transferencia de datos electrónicos no personales a terceros países

1. Los datos de salud electrónicos no personales proporcionados por los organismos de acceso a datos de salud a un usuario de datos de salud de un tercer país en virtud de un permiso de datos expedido de conformidad con el artículo 68 del presente Reglamento o una petición de datos de salud aprobada de conformidad con el artículo 69 del presente Reglamento, a participantes autorizados de un tercer país o a una organización internacional, y basados en datos de salud electrónicos de una persona física incluidos en una de las categorías a que se refiere el artículo 51 del presente Reglamento se considerarán muy sensibles en el sentido del artículo 5, apartado 13, del Reglamento (UE) 2022/868, cuando la transferencia de dichos datos electrónicos no personales a terceros países presente un riesgo de reidentificación por medios que vayan más allá de los que razonablemente puedan utilizarse, en particular habida cuenta del número limitado de personas físicas a las que se refieran dichos datos, del hecho de que estén geográficamente dispersas o de los avances tecnológicos esperados en un futuro próximo.

2. Las medidas de protección para las categorías de datos mencionadas en el apartado 1 del presente artículo se detallarán en un acto delegado a que se refiere el artículo 5, apartado 13, del Reglamento (UE) 2022/868.

Artículo 89

Acceso gubernamental internacional a datos de salud electrónicos no personales

1. Las autoridades de salud digital, los organismos de acceso a datos de salud, los participantes autorizados en las infraestructuras transfronterizas contempladas en los artículos 23 y 75 y los usuarios de datos de salud adoptarán todas las medidas técnicas, jurídicas y organizativas razonables, lo que incluye acuerdos contractuales, a fin de impedir la transferencia de datos de salud electrónicos no personales conservados en la Unión a un tercer país o a una organización internacional, incluso para un acceso gubernamental en un tercer país, cuando dicha transferencia entre en conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro de que se trate.

2. Las sentencias de los órganos jurisdiccionales de un tercer país o las decisiones de las autoridades administrativas de un tercer país por las que se exija a una autoridad de salud digital, un organismo de acceso a datos de salud o los usuarios de datos de salud transferir datos de salud electrónicos no personales conservados en la Unión e incluidos en el ámbito de aplicación del presente Reglamento, o dar acceso a tales datos, solo se reconocerán o ejecutarán de cualquier forma si se basan en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el tercer país solicitante y la Unión o entre el tercer país solicitante y un Estado miembro.

3. A falta del acuerdo internacional a que se refiere el apartado 2, cuando una autoridad de salud digital, un organismo de acceso a datos de salud o un usuario de datos de salud sea el destinatario de una resolución o sentencia de un órgano jurisdiccional de un tercer país o una decisión de una autoridad administrativa de un tercer país por la que se le exija transferir datos no personales conservados en la Unión e incluidos en el ámbito de aplicación del presente Reglamento, o dar acceso a tales datos, y el cumplimiento de dicha resolución, sentencia o decisión entrañe el riesgo de que el destinatario entre en conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro de que se trate, la transferencia o el acceso a tales datos por dicho órgano jurisdiccional o autoridad administrativa de un tercer país únicamente tendrá lugar cuando:

a) el ordenamiento jurídico del tercer país exija que se expongan los motivos y la proporcionalidad de la resolución, sentencia o decisión y que dicha resolución, sentencia o decisión sea de carácter específico, por ejemplo, estableciendo un vínculo suficiente con determinadas personas sospechosas o infracciones;

b) la oposición motivada del destinatario requiera ser examinada por un órgano jurisdiccional competente del tercer país, y

c) el órgano jurisdiccional competente del tercer país que dicte la resolución o sentencia o examine la decisión de una autoridad administrativa esté facultado por el Derecho nacional del tercer país en cuestión para tener debidamente en cuenta los intereses jurídicos pertinentes del proveedor de los datos protegidos por el Derecho de la Unión o por el Derecho nacional del Estado miembro pertinente.

4. Si se cumplen las condiciones establecidas en los apartados 2 o 3, la autoridad de salud digital, un organismo de acceso a datos de salud o una organización de cesión altruista de datos proporcionará la cantidad mínima de datos permitida en respuesta a una petición, sobre la base de una interpretación razonable de tal petición.

5. Antes de dar cumplimiento a la petición, las autoridades de salud digital, los organismos de acceso a datos de salud y los usuarios de datos de salud informarán al tenedor de datos de salud de que una autoridad administrativa de un tercer país ha presentado una solicitud de acceso a sus datos, excepto en los casos en que la solicitud sirva a fines de aplicación de la ley y mientras sea necesario el cumplimiento para preservar la eficacia de las actividades correspondientes de aplicación de la ley.

Artículo 90

Condiciones adicionales para la transferencia de datos de salud electrónicos personales a un tercer país o a una organización internacional

La transferencia de datos de salud electrónicos personales a un tercer país o a una organización internacional se concederá de conformidad con el capítulo V del Reglamento (UE) 2016/679. Los Estados miembros podrán mantener o introducir condiciones adicionales sobre el acceso internacional a los datos de salud electrónicos personales y su transferencia, incluidas limitaciones, de conformidad con el artículo 9, apartado 4, del Reglamento (UE) 2016/679, además de los requisitos establecidos en el artículo 24, apartado 3, y en el artículo 75, apartado 5, del presente Reglamento y en el capítulo V del Reglamento (UE) 2016/679.

Artículo 91

Solicitudes de acceso a datos de salud y peticiones de datos de salud por terceros países

1. Sin perjuicio de lo dispuesto en los artículos 67, 68 y 69, las solicitudes de acceso a datos de salud y las peticiones de datos de salud presentadas por un solicitante de datos de salud establecido en un tercer país serán admisibles por los organismos de acceso a datos de salud y el servicio de acceso a datos de salud de la Unión si el tercer país de que se trate:

a) es un participante autorizado basándose en que dispone de un punto de contacto nacional para uso secundario incluido en un acto de ejecución a que se refiere el artículo 75, apartado 5, o

b) permite a los solicitantes de datos de salud de la Unión acceder a datos de salud electrónicos en ese tercer país en condiciones que no sean más restrictivas que las establecidas en el presente Reglamento y que, por lo tanto, dicho acceso esté incluido en un acto de ejecución del apartado 2 del presente artículo.

2. Mediante actos de ejecución, la Comisión podrá determinar que un tercer país cumple el requisito establecido en el apartado 1, letra b), del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2. La Comisión hará pública la lista de actos de ejecución adoptados en virtud del presente apartado.

3. La Comisión hará un seguimiento de la evolución en terceros países y organizaciones internacionales que pueda afectar a la aplicación de los actos de ejecución adoptados con arreglo al apartado 2, y establecerá una revisión periódica de la aplicación del presente artículo.

Cuando la Comisión considere que un tercer país ha dejado de cumplir el requisito establecido en el apartado 1, letra b), del presente artículo, adoptará un acto de ejecución por el que se derogue el acto de ejecución mencionado en el apartado 2 del presente artículo relativo a dicho tercer país que disfruta de acceso. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

CAPÍTULO VI

GOBERNANZA Y COORDINACIÓN EUROPEA

Artículo 92

Consejo del Espacio Europeo de Datos de Salud

1. Se crea un Consejo del Espacio Europeo de Datos de Salud («Consejo del EEDS») para facilitar la cooperación y el intercambio de información entre los Estados miembros y la Comisión. El Consejo del EEDS estará integrado por dos representantes por Estado miembro, a saber, un representante para fines de uso primario y otro para fines de uso secundario, designados por cada Estado miembro. Cada Estado miembro dispondrá de un voto. Los miembros del Consejo del EEDS se comprometerán a actuar en interés público y de manera independiente.

2. Las reuniones del Consejo del EEDS estarán copresididas por un representante de la Comisión y uno de los representantes de los Estados miembros a que se refiere el apartado 1.

3. Se invitará a las autoridades de vigilancia del mercado a que se refiere el artículo 43, al CEPD y al Supervisor Europeo de Protección de Datos, a la Agencia Europea de Medicamentos, al Centro Europeo para la Prevención y el Control de las Enfermedades y a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) a asistir a las reuniones cuando el Consejo del EEDS lo considere pertinente.

4. El Consejo del EEDS podrá invitar a asistir a sus reuniones a autoridades nacionales, expertos y observadores, así como a instituciones, órganos y organismos de la Unión, además de los referidos en el apartado 3, e infraestructuras de investigación y otras infraestructuras similares.

5. El Consejo del EEDS podrá cooperar con expertos externos, en su caso.

6. Dependiendo de las funciones relacionadas con el uso de datos de salud electrónicos, el Consejo del EEDS podrá trabajar en subgrupos para determinados temas, en los que estarán representadas las autoridades de salud digital o los organismos de acceso a datos de salud. Esos subgrupos prestarán asistencia al Consejo del EEDS con conocimientos especializados específicos y, en caso necesario, podrán celebrar reuniones conjuntas.

7. El Consejo del EEDS adoptará su reglamento interno y un código de conducta, a propuesta de la Comisión. Dicho reglamento interno establecerá la composición, organización, funcionamiento y cooperación de los subgrupos a que se refiere el apartado 6 del presente artículo y la cooperación del Consejo del EEDS con el foro de partes interesadas a que se refiere el artículo 93.

El Consejo del EEDS adoptará decisiones por consenso en la medida de lo posible. Si no puede alcanzarse un consenso, el Consejo del EEDS adoptará decisiones por mayoría de dos tercios de los Estados miembros.

8. El Consejo del EEDS cooperará con otros organismos, entidades y expertos pertinentes, como el Comité Europeo de Innovación en materia de Datos creado por el artículo 29 del Reglamento (UE) 2022/868, las autoridades competentes designadas de conformidad con el artículo 37 del Reglamento (UE) 2023/2854, los organismos de supervisión designados de conformidad con el artículo 46 *ter* del Reglamento (UE) n.º 910/2014, el CEPD creado por el artículo 68 del Reglamento (UE) 2016/679, los organismos de ciberseguridad, incluida ENISA, y la Nube Europea de la Ciencia Abierta, a fin de lograr soluciones avanzadas para un uso de datos que sean fácil de encontrar, accesibles, interoperables y reutilizables (FAIR) en la investigación y la innovación.

9. El Consejo del EEDS estará asistido por una secretaría proporcionada por la Comisión.

10. El Consejo del EEDS publicará las fechas de sus reuniones y las actas de sus deliberaciones, así como un informe bienal de actividad.

11. La Comisión adoptará, mediante actos de ejecución, las medidas necesarias para el establecimiento y las operaciones del Consejo del EEDS. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 98, apartado 2.

Artículo 93

Foro de partes interesadas

1. Se crea un foro de partes interesadas con el fin de facilitar el intercambio de información y promover la cooperación entre las partes interesadas en relación con la aplicación del presente Reglamento.

2. El foro de partes interesadas tendrá una composición equilibrada y estará integrado por partes interesadas pertinentes, incluidos representantes de organizaciones de pacientes, profesionales sanitarios, sector empresarial, organizaciones de consumidores, investigadores científicos y el mundo académico y representará sus puntos de vista. Cuando haya intereses comerciales representados en el foro de partes interesadas, la representación de tales intereses se hará con base a una combinación equilibrada de grandes empresas, pymes y empresas emergentes. Las funciones del foro de partes interesadas englobarán por igual el uso primario y el uso secundario.

3. Los miembros del foro de partes interesadas serán designados por la Comisión tras una convocatoria pública de manifestaciones de interés y un procedimiento de selección transparente. Los miembros del foro de partes interesadas harán una declaración anual de intereses, que se pondrá a disposición del público y se actualizará, cuando proceda.

4. El foro de partes interesadas podrá crear subgrupos permanentes o temporales, según proceda, a fin de examinar cuestiones específicas relacionadas con los objetivos del presente Reglamento. El foro de partes interesadas adoptará su reglamento interno.

5. El foro de partes interesadas celebrará reuniones periódicas que serán presididas por un representante de la Comisión.

6. El foro de partes interesadas elaborará un informe anual de sus actividades. Dicho informe se pondrá a disposición del público.

Artículo 94

Funciones del Consejo del EEDS

1. El Consejo del EEDS tendrá las siguientes funciones relacionadas con el uso primario, de conformidad con los capítulos II y III:

a) ayudar a los Estados miembros a coordinar las prácticas de las autoridades de salud digital;

b) presentar contribuciones por escrito e intercambiar buenas prácticas sobre cuestiones relacionadas con la coordinación de la aplicación a nivel de los Estados miembros, teniendo en cuenta el nivel regional y local, del presente Reglamento y de los actos delegados y de ejecución adoptados en virtud de él, en particular por lo que respecta a:

   i) las disposiciones de los capítulos II y III,

   ii) el desarrollo de servicios en línea que faciliten un acceso seguro, incluida una identificación electrónica segura, a los datos de salud electrónicos para los profesionales sanitarios y las personas físicas,

   iii) otros aspectos relacionados con el uso primario;

c) facilitar la cooperación entre las autoridades de salud digital a través del desarrollo de las capacidades, mediante el establecimiento del marco de los informes de actividad a que se refiere el artículo 20 y el intercambio de información;

d) compartir información entre sus miembros sobre los riesgos que entrañan los sistemas HCE y los incidentes graves, así como la gestión de dichos riesgos e incidentes;

e) facilitar el intercambio de puntos de vista sobre el uso primario con el foro de partes interesadas a que se refiere el artículo 93, así como con los reguladores y los responsables políticos del sector sanitario.

2. El Consejo del EEDS tendrá las siguientes funciones relacionadas con el uso secundario de conformidad con el capítulo IV:

a) ayudar a los Estados miembros a coordinar las prácticas de los organismos de acceso a datos de salud en la aplicación de las disposiciones establecidas en el capítulo IV, a fin de garantizar una aplicación coherente del presente Reglamento;

b) presentar contribuciones por escrito e intercambiar buenas prácticas sobre cuestiones relacionadas con la coordinación de la aplicación a nivel de los Estados miembros del presente Reglamento y de los actos delegados y de ejecución adoptados en virtud de él, en particular por lo que respecta a:

   i) la aplicación de las reglas de acceso a los datos de salud electrónicos,

   ii) las especificaciones técnicas o las normas existentes relativas a los requisitos establecidos en el capítulo IV,

   iii) los incentivos para promover la calidad de los datos y la mejora de la interoperabilidad,

   iv) las políticas relativas a las tasas que deben cobrar los organismos de acceso a datos de salud y los tenedores de datos de salud,

   v) las medidas para proteger los datos personales de los profesionales sanitarios que dispensan tratamiento a personas físicas,

   vi) otros aspectos del uso secundario;

c) crear, en consulta y cooperación con las partes interesadas pertinentes, incluidos los representantes de los pacientes, los profesionales sanitarios y los investigadores, directrices para ayudar a los usuarios de datos de salud a cumplir las obligaciones que les incumben con arreglo al artículo 61, apartado 5, en particular para determinar si sus hallazgos son clínicamente significativos;

d) facilitar la cooperación entre los organismos de acceso a datos de salud mediante el desarrollo de las capacidades, estableciendo el marco para la presentación de informes de actividad a que se refiere el artículo 59, apartado 1, y el intercambio de información;

e) compartir información sobre los riesgos y los incidentes relacionados con el uso secundario, así como la gestión de dichos riesgos e incidentes;

f) facilitar el intercambio de opiniones sobre el uso secundario con el foro de partes interesadas a que se refiere el artículo 93, así como con los tenedores de datos de salud, los usuarios de datos de salud, los reguladores y los responsables políticos del sector sanitario.

Artículo 95

Grupos rectores de MiSalud@UE y DatosSalud@UE

1. Se crea el grupo rector MiSalud@UE y el grupo rector DatosSalud@UE (en lo sucesivo, «grupos rectores») para las infraestructuras transfronterizas contempladas en los artículos 23 y 75. Cada grupo rector estará compuesto por un representante por Estado miembro designado de entre los puntos de contacto nacionales pertinentes.

2. Los grupos rectores adoptarán decisiones operativas relativas al desarrollo y el funcionamiento de MiSalud@UE y DatosSalud@UE.

3. Los grupos rectores adoptarán sus decisiones por consenso. Cuando no pueda alcanzarse un consenso, la decisión se adoptará por mayoría de dos tercios de sus miembros. Para la adopción de las decisiones, cada Estado miembro tendrá un voto.

4. Los grupos rectores adoptarán su reglamento interno, que establecerá su composición, organización, funcionamiento y cooperación.

5. Podrá invitarse a otros participantes autorizados a intercambiar información y puntos de vista sobre cuestiones pertinentes relacionadas con MiSalud@UE y DatosSalud@UE. Cuando se invite a dichos participantes autorizados, estos tendrán la condición de observador.

6. Las partes interesadas y los terceros pertinentes, incluidos los representantes de los pacientes, de los profesionales sanitarios, de los consumidores y del sector empresarial, podrán ser invitados a asistir a las reuniones de los grupos rectores en calidad de observadores.

7. Los grupos rectores elegirán a los presidentes de sus reuniones.

8. Los grupos rectores estarán asistidos por una secretaría proporcionada por la Comisión.

Artículo 96

Funciones y responsabilidades de la Comisión en relación con el funcionamiento del EEDS

1. Además de su función en la puesta a disposición de datos de salud electrónicos en poder de las instituciones, órganos y organismos de la Unión, de conformidad con los artículos 55, 56 y artículo 75, apartado 2, y sus funciones en virtud del capítulo III, especialmente el artículo 40, la Comisión desarrollará, mantendrá, alojará y explotará las infraestructuras y los servicios centrales necesarios para apoyar el funcionamiento del EEDS, para todas las entidades conectadas pertinentes, por medio de:

a) un mecanismo interoperable y transfronterizo de identificación y autenticación para las personas físicas y los profesionales sanitarios, de conformidad con el artículo 16, apartados 3 y 4;

b) los servicios centrales y las infraestructuras para la salud digital de MiSalud@UE, de conformidad con el artículo 23, apartado 1;

c) comprobaciones del cumplimiento para conectar a los participantes autorizados a MiSalud@UE, de conformidad con el artículo 23, apartado 9;

d) los servicios e infraestructuras sanitarios digitales transfronterizos complementarios a que se refiere el artículo 24, apartado 1;

e) como parte de DatosSalud@UE, un servicio para presentar solicitudes de acceso a datos de salud con la intención de acceder a datos de salud electrónicos en poder de tenedores de datos de salud en más de un Estado miembro o de otros participantes autorizados en DatosSalud@UE y enviar automáticamente las solicitudes de acceso a datos de salud a los puntos de contacto pertinentes, de conformidad con el artículo 67, apartado 3;

f) los servicios centrales y las infraestructuras de DatosSalud@UE, de conformidad con el artículo 75, apartados 7 y 8;

g) un entorno de tratamiento seguro, de conformidad con el artículo 75, apartado 9, en el que los organismos de acceso a datos de salud puedan decidir poner los datos a disposición con arreglo al artículo 68, apartado 8;

h) comprobaciones del cumplimiento para conectar a los participantes autorizados a DatosSalud@UE, de conformidad con el artículo 75, apartado 5;

i) un catálogo federado de conjuntos de datos de la UE que conecte los catálogos de conjuntos de datos nacionales, de conformidad con el artículo 79;

j) una secretaría para el Consejo del EEDS, de conformidad con el artículo 92, apartado 9;

k) una secretaría para los grupos rectores, de conformidad con el artículo 95, apartado 8.

2. Los servicios a que se refiere el apartado 1 del presente artículo cumplirán normas de calidad suficientes en términos de disponibilidad, seguridad, capacidad, interoperabilidad, mantenimiento, seguimiento y desarrollo para garantizar que el EEDS funcione de manera eficaz. La Comisión prestará dichos servicios de conformidad con las decisiones operativas de los grupos rectores pertinentes que dispone el artículo 95.

3. La Comisión preparará un informe sobre las infraestructuras y los servicios de apoyo al EEDS que ella le proporcione de conformidad con el apartado 1, con periodicidad bienal y lo publicará.

CAPÍTULO VII

DELEGACIÓN DE PODERES Y PROCEDIMIENTO DE COMITÉ

Artículo 97

Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar actos delegados mencionados en el artículo 14, apartado 2, el artículo 49, apartado 4, y el artículo 78, apartado 5, se otorgan a la Comisión por un período de tiempo indefinido a partir del 25 de marzo de 2025.

3. La delegación de poderes mencionada en el artículo 14, apartado 2, el artículo 49, apartado 4, y el artículo 78, apartado 5, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 14, apartado 2, del artículo 49, apartado 4, y del artículo 78, apartado 5, entrarán en vigor únicamente si, en un plazo de tres meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 98

Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

CAPÍTULO VIII

DISPOSICIONES VARIAS

Artículo 99

Sanciones

Los Estados miembros establecerán el régimen de las sanciones aplicables a cualquier infracción del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas según lo dispuesto en los artículos 63 y 64, y adoptarán todas las medidas necesarias para garantizar su ejecución. Tales sanciones serán efectivas, proporcionadas y disuasorias. Los Estados miembros comunicarán a la Comisión el régimen establecido y las medidas adoptadas, a más tardar el 26 de marzo de 2027, y le notificarán sin demora toda modificación posterior.

Los Estados miembros tendrán en cuenta los siguientes criterios indicativos y no exhaustivos para la imposición de sanciones por infracciones del presente Reglamento, cuando proceda:

a) la naturaleza, gravedad, magnitud y duración de la infracción;

b) cualquier medida adoptada por el infractor para atenuar o reparar el perjuicio causado por la infracción;

c) cualquier infracción anterior del infractor;

d) los beneficios financieros obtenidos o las pérdidas evitadas por el infractor debido a la infracción, en la medida en que dichos beneficios o pérdidas puedan calcularse de forma fiable;

e) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso;

f) el volumen de negocio anual del infractor en la Unión durante el ejercicio financiero anterior.

Artículo 100

Derecho a recibir una indemnización

Toda persona física o jurídica que haya sufrido daños materiales o morales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir una indemnización de conformidad con el Derecho de la Unión y nacional.

Artículo 101

Representación de personas físicas

La persona física que considere que se han vulnerado los derechos que le reconoce el presente Reglamento tendrá derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro constituida con arreglo al Derecho nacional, que tenga objetivos estatutarios de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación o ejerza los derechos a que se refieren los artículos 21 y 81.

Artículo 102

Evaluación, revisión e informe de situación

1. A más tardar el 26 de marzo de 2033, la Comisión realizará una evaluación selectiva del presente Reglamento y presentará un informe sobre sus principales conclusiones al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo, y al Comité de las Regiones, acompañado, en su caso, de una propuesta de modificación. Dicha evaluación incluirá los elementos siguientes:

a) las posibilidades de seguir ampliando la interoperabilidad entre los sistemas HCE y los servicios de acceso a datos de salud electrónicos distintos de los establecidos por los Estados miembros;

b) la necesidad de actualizar las categorías de datos a que se refiere el artículo 51 y los fines a que se refiere el artículo 53, apartado 1;

c) la aplicación y el uso por parte de las personas físicas de los mecanismos de autoexclusión del uso secundario a que se refiere el artículo 71, en particular sobre las repercusiones de dichos mecanismos en la salud pública, la investigación científica y los derechos fundamentales;

d) el uso y aplicación de cualquier medida más estricta introducida con arreglo al artículo 51, apartado 4;

e) el ejercicio y aplicación del derecho a que se refiere el artículo 8;

f) una valoración del marco de certificación de los sistemas HCE establecido en el capítulo III y la necesidad de introducir más herramientas en relación con la evaluación de la conformidad;

g) una evaluación del funcionamiento del mercado interior para los sistemas HCE;

h) una evaluación de los costes y beneficios de la aplicación de las disposiciones relativas al uso secundario establecidas en el capítulo IV;

i) la aplicación de tasas como dispone el artículo 62.

2. A más tardar el 26 de marzo de 2035, la Comisión realizará una evaluación global del presente Reglamento y presentará un informe sobre sus principales conclusiones al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo, y al Comité de las Regiones, acompañado, en su caso, de una propuesta de modificación u otras medidas apropiadas. Esa evaluación incluirá una valoración de la eficiencia y el funcionamiento de los sistemas que proporcionan acceso a los datos de salud electrónicos para su posterior tratamiento, efectuada sobre la base del Derecho de la Unión o nacional a que se refiere el artículo 1, apartado 7, con respecto a sus repercusiones en la aplicación del presente Reglamento.

3. Los Estados miembros proporcionarán a la Comisión la información necesaria para la elaboración de los informes a que se refieren los apartados 1 y 2 y la Comisión tendrá debidamente en cuenta esa información en dichos informes.

4. Cada año después del 25 de marzo de 2025 hasta el final del año en el que todas las disposiciones del presente Reglamento sean aplicables tal como dispone el artículo 105, la Comisión presentará un informe de situación al Consejo sobre los preparativos para la plena aplicación del presente Reglamento. Dicho informe de situación contendrá información sobre el grado de progreso y la preparación de los Estados miembros en relación con la aplicación del presente Reglamento, incluida una valoración de la viabilidad de alcanzar los plazos establecidos en el artículo 105, y también podrá contener recomendaciones a los Estados miembros para mejorar la preparación para la aplicación del presente Reglamento.

Artículo 103

Modificación de la Directiva 2011/24/UE

Se suprime el artículo 14 de la Directiva 2011/24/UE con efectos a partir del 26 de marzo de 2031.

Artículo 104

Modificación del Reglamento (UE) 2024/2847

El Reglamento (UE) 2024/2847 se modifica como sigue:

1) En el artículo 13, el apartado 4 se sustituye por el texto siguiente:

«4. Al introducir en el mercado un producto con elementos digitales, el fabricante incluirá la evaluación de riesgos de ciberseguridad a que se refiere el apartado 3 del presente artículo en la documentación técnica exigida en virtud del artículo 31 y el anexo VII. En el caso de los productos con elementos digitales a que se refieren el artículo 12 y el artículo 32, apartado 5 *bis*, a los que también se apliquen otros actos jurídicos de la Unión, la evaluación de los riesgos de ciberseguridad podrá formar parte de la evaluación de riesgos exigida por dichos actos jurídicos de la Unión. Cuando determinados requisitos esenciales de ciberseguridad no sean aplicables al producto con elementos digitales, el fabricante incluirá una justificación clara a tal efecto en la documentación técnica citada.».

2) En el artículo 31, el apartado 3 se sustituye por el texto siguiente:

«3. En el caso de los productos con elementos digitales a que se refieren el artículo 12 y el artículo 32, apartado 5 *bis*, a los que también se apliquen otros actos jurídicos de la Unión que prevean documentación técnica, se elaborará una única documentación técnica que contenga la información a que hace referencia el anexo VII del presente Reglamento y la información obligatoria según esos otros actos jurídicos de la Unión.».

3) En el artículo 32, se inserta el apartado siguiente:

«5 *bis*. Los fabricantes de productos con elementos digitales considerados sistemas HCE con arreglo al Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo (*) demostrarán la conformidad con los requisitos esenciales establecidos en el anexo I del presente Reglamento mediante el procedimiento de evaluación de la conformidad pertinente previsto en el capítulo III del Reglamento (UE) 2025/327.

(*) Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847 (DO L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj).».

CAPÍTULO IX

APLICACIÓN DIFERIDA Y DISPOSICIONES TRANSITORIAS Y FINALES

Artículo 105

Entrada en vigor y aplicación

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será aplicable a partir del 26 de marzo de 2027.

No obstante, los artículos 3 a 15, el artículo 23, apartados 2 a 6, los artículos 25, 26, 27, 47, 48 y 49 serán aplicables como sigue:

a) a partir del 26 de marzo de 2029, a las categorías prioritarias de datos de salud electrónicos personales a que se refiere el artículo 14, apartado 1, letras a), b) y c), y a los sistemas HCE destinados por el fabricante al tratamiento de esas categorías de datos;

b) a partir del 26 de marzo de 2031, a las categorías prioritarias de datos de salud electrónicos personales a que se refiere el artículo 14, apartado 1, letras d), e) y f), y a los sistemas HCE destinados por el fabricante al tratamiento de esas categorías de datos;

c) a partir de un año desde la fecha establecida en un acto delegado adoptado en virtud del artículo 14, apartado 2, para cada modificación de las principales características de los datos de salud electrónicos personales establecidas en el anexo I, siempre que dicha fecha sea posterior a la fecha de aplicación a que se refieren las letras a) y b) del presente párrafo para las categorías de datos de salud electrónicos personales de que se trate.

El capítulo III será aplicable a los sistemas HCE puestos en servicio en la Unión a que se refiere el artículo 26, apartado 2, a partir del 26 de marzo de 2031.

El capítulo IV será aplicable a partir del 26 de marzo de 2029. No obstante, el artículo 55, apartado 6, el artículo 70, el artículo 73, apartado 5, el artículo 75, apartados 1 y 12, el artículo 77, apartado 4, y el artículo 78, apartado 6, serán aplicables a partir del 26 de marzo de 2027, el artículo 51, apartado 1, letras b), f), g), m) y p), será aplicable a partir del 26 de marzo de 2031, y el artículo 75, apartado 5, será aplicable a partir del 26 de marzo de 2035.

Los actos de ejecución a que se refieren el artículo 13, apartado 3, el artículo 15, apartado 1, el artículo 23, apartado 4, y el artículo 36, apartado 1, serán aplicables a partir de las fechas a que se refiere el párrafo tercero del presente artículo dependiendo de las categorías de datos de salud electrónicos personales a que se refiere el artículo 14, apartado 1, letras a), b) y c), o el artículo 14, apartado 1, letras d), e) y f), respectivamente.

Los actos de ejecución a que se refieren el artículo 70, el artículo 73, apartado 5, el artículo 75, apartado 12, el artículo 77, apartado 4, y el artículo 78, apartado 6, serán aplicables a partir del 26 de marzo de 2029.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Estrasburgo, el 11 de febrero de 2025.

Por el Parlamento Europeo	*Por el Consejo*
La Presidenta	*El Presidente*
R. METSOLA	A. SZŁAPKA

ANEXO I

Principales características de las categorías prioritarias de datos de salud electrónicos personales para uso primario

Categoría de datos de salud electrónicos	Principales características de los datos de salud electrónicos incluidos en la categoría
1. Historias clínicas resumidas de pacientes	Datos de salud electrónicos que incluyen hechos clínicos importantes relacionados con una persona física identificada y que son esenciales para prestarle una asistencia sanitaria segura y eficiente. La siguiente información forma parte de una historia clínica resumida del paciente: 1. Datos personales. 2. Información de contacto. 3. Información sobre los seguros. 4. Alergias. 5. Alertas médicas. 6. Información sobre vacunación/inmunización, posiblemente en forma de carnet de vacunación. 7. Problemas de salud actuales, resueltos, cerrados o inactivos, indicados mediante una codificación de la clasificación internacional. 8. Información textual relacionada con la historia clínica. 9. Productos sanitarios e implantes. 10. Procedimientos médicos o asistenciales. 11. Estado funcional. 12. Medicamentos actuales y pasados que convenga indicar. 13. Observaciones sobre los antecedentes sociales relacionadas con la salud. 14. Historial de embarazos. 15. Datos proporcionados por el paciente. 16. Resultados de la observación referentes al estado de salud. 17. Plan de asistencia. 18. Información sobre una enfermedad rara, por ejemplo, detalles sobre los efectos o las características de la enfermedad.
2. Recetas electrónicas	Datos de salud electrónicos que constituyen una receta de un medicamento, tal como se define en el artículo 3, letra k), de la Directiva 2011/24/UE.
3. Dispensaciones electrónicas	Información sobre el suministro de un medicamento a una persona física por parte de una farmacia sobre la base de una receta electrónica.
4. Estudios de diagnóstico por imagen e informes de imágenes correspondientes	Datos de salud electrónicos relacionados con el uso de tecnologías que se utilizan para observar el cuerpo humano con el fin de prevenir, diagnosticar, vigilar o tratar problemas de salud, o producidos por dichas tecnologías.
5. Resultados de pruebas diagnósticas, incluidos resultados de laboratorio y otros resultados de diagnóstico e informes correspondientes	Datos de salud electrónicos que reflejan los resultados de estudios realizados, en particular, a través de diagnósticos *in vitro*, como, por ejemplo, bioquímica clínica, hematología, medicina transfusional, microbiología, inmunología y otros, incluidos, en su caso, informes que corroboran la interpretación de los resultados.
6. Informes de alta hospitalaria	Datos de salud electrónicos relacionados con una consulta médica o un acto de asistencia que incluyen información esencial sobre el ingreso, el tratamiento y el alta de una persona física.

ANEXO II

Requisitos esenciales exigibles a los componentes armonizados de programa informático de los sistemas HCE y a los productos para los que se declare la interoperabilidad con los sistemas HCE

Los requisitos esenciales establecidos en el presente anexo se aplicarán *mutatis mutandis* a los productos sanitarios, productos sanitarios para diagnóstico *in vitro*, sistemas de IA y aplicaciones de bienestar para los que se declara la interoperabilidad con los sistemas HCE.

1. Requisitos generales

1.1. Los componentes armonizados de programa informático de un sistema HCE alcanzarán el funcionamiento previsto conforme a lo previsto por su fabricante y deberán diseñarse y fabricarse para que, en condiciones normales de uso, se adecúen a su finalidad prevista y su uso no ponga en peligro la seguridad de los pacientes.

1.2. Los componentes armonizados de programa informático de un sistema HCE se diseñarán y desarrollarán de manera que el sistema HCE pueda suministrarse e instalarse teniendo en cuenta las instrucciones y la información proporcionadas por el fabricante, sin que sus características y funcionamiento se vean afectados negativamente durante su uso previsto.

1.3. Un sistema HCE se diseñará y desarrollará de manera que sus características de interoperabilidad, seguridad y protección respeten los derechos de las personas físicas, en consonancia con la finalidad prevista del sistema, tal como se establece en el capítulo II.

1.4. Los componentes armonizados de programa informático de un sistema HCE destinado a funcionar en combinación con otros productos, incluidos productos sanitarios, se diseñará y fabricará de manera que su interoperabilidad y compatibilidad sean fiables y seguras, y los datos de salud electrónicos personales puedan compartirse entre el producto y el sistema HCE en relación con esos componentes armonizados de programa informático de un sistema HCE.

2. Requisitos de interoperabilidad

2.1. Cuando un sistema HCE esté diseñado para almacenar o intermediar datos de salud electrónicos personales, proporcionará una interfaz que permita acceder a los datos de salud electrónicos personales tratados por él en el formato europeo de intercambio de historias clínicas electrónicas, a través del componente de programa informático europeo de interoperabilidad para sistemas HCE.

2.2. Cuando un sistema HCE esté diseñado para almacenar o intermediar datos de salud electrónicos personales, podrá recibir datos de salud electrónicos personales en el formato europeo de intercambio de historias clínicas electrónicas, a través del componente de programa informático europeo de interoperabilidad para sistemas HCE.

2.3. Cuando un sistema HCE esté diseñado para proporcionar acceso a datos de salud electrónicos personales, podrá recibir datos de salud electrónicos personales en el formato europeo de intercambio de historias clínicas electrónicas, a través del componente de programa informático europeo de interoperabilidad para sistemas HCE.

2.4. Un sistema HCE que incluya una funcionalidad para introducir datos de salud electrónicos personales estructurados permitirá la introducción de datos con una granularidad suficiente para permitir el suministro de los datos de salud electrónicos personales introducidos en el formato europeo de intercambio de historias clínicas electrónicas.

2.5. Los componentes armonizados de programa informático de un sistema HCE no incluirán características que prohíban o limiten el acceso autorizado, el intercambio electrónico de datos de salud personales o el uso de estos datos para fines permitidos, o que impongan una carga indebida a tales efectos.

2.6. Los componentes armonizados de programa informático de un sistema HCE no incluirán características que prohíban o limiten la exportación autorizada de datos de salud electrónicos personales con el fin de sustituir el sistema HCE por otro producto, o que impongan una carga indebida a tales efectos.

3. Requisitos de seguridad y de registro

3.1. Todo sistema HCE diseñado para ser utilizado por profesionales sanitarios incluirá mecanismos fiables para la identificación y autenticación de los profesionales sanitarios.

3.2. El componente de programa informático europeo de registro de un sistema HCE diseñado para posibilitar el acceso de los prestadores de asistencia sanitaria u otras personas a datos de salud electrónicos personales incluirá mecanismos de registro suficientes que graben, como mínimo, la siguiente información sobre cada evento o grupo de eventos de acceso:

a) la identificación del prestador de asistencia sanitaria o de otras personas que hayan accedido a los datos de salud electrónicos personales;

b) la identificación de la persona o personas físicas concretas que hayan accedido a los datos de salud electrónicos personales;

c) las categorías de datos a los que se haya accedido;

d) la hora y fecha de acceso;

e) el origen u orígenes de los datos.

3.3. Los componentes armonizados de programa informático del sistema HCE incluirán herramientas o mecanismos para revisar y analizar los datos de los registros, o deberán permitir la conexión y la utilización de programas informáticos externos para los mismos fines.

3.4. Los componentes armonizados de programa informático de un sistema HCE que almacene datos de salud electrónicos personales permitirán diferentes períodos de conservación y derechos de acceso que tengan en cuenta el origen y las categorías de tales datos.

ANEXO III

Documentación técnica

La documentación técnica a que se refiere el artículo 37 contendrá como mínimo la siguiente información, en función de los componentes armonizados de programa informático de un sistema HCE del correspondiente sistema HCE:

1. Una descripción pormenorizada del sistema HCE que incluya:
   a) su finalidad prevista, la fecha y la versión del sistema HCE;
   b) las categorías de datos de salud electrónicos personales para cuyo tratamiento el sistema HCE ha sido diseñado;
   c) la manera en que el sistema HCE interactúa, o puede utilizarse para interactuar, con equipos o programas informáticos que no forman parte del propio sistema;
   d) las versiones de los programas y los soportes intermedios (*firmware*) pertinentes y cualquier requisito relativo a la actualización de las versiones;
   e) la descripción de todas las formas en las que el sistema HCE se ha introducido en el mercado o se ha puesto en servicio;
   f) la descripción del equipo informático en el que se prevé que opere el sistema HCE;
   g) una descripción de la arquitectura del sistema que explique cómo se apoyan o se alimentan mutuamente los componentes de los programas informáticos y cómo se integran en el tratamiento general, que incluya, en su caso, etiquetas con representaciones gráficas (por ejemplo, diagramas y dibujos), así como una indicación clara de las partes o componentes de programa informático clave y una explicación suficiente para comprender los dibujos y diagramas;
   h) las especificaciones técnicas del sistema HCE, tales como las características, las dimensiones y los atributos de funcionamiento, así como otras variantes o configuraciones y accesorios que figuran normalmente en las especificaciones del producto disponibles para el usuario, por ejemplo en folletos, catálogos y publicaciones similares, incluida una descripción pormenorizada de las estructuras de datos, el almacenamiento y la entrada/salida de datos;
   i) una descripción de todo cambio introducido en el sistema a lo largo de su ciclo de vida;
   j) las instrucciones de uso para el usuario y, cuando proceda, las instrucciones de instalación.
2. Una descripción pormenorizada del sistema que se utiliza para evaluar el funcionamiento del sistema HCE, cuando proceda.
3. Las referencias a las especificaciones comunes utilizadas de conformidad con el artículo 36 y con respecto a las cuales se declara la conformidad.
4. Los resultados y los análisis críticos de todas las verificaciones y pruebas de validación realizadas para demostrar la conformidad del sistema HCE con los requisitos establecidos en el capítulo III, en particular los requisitos esenciales aplicables.
5. Una copia de la ficha informativa mencionada en el artículo 38.
6. Una copia de la declaración UE de conformidad.

ANEXO IV

Declaración UE de conformidad

La declaración UE de conformidad para los componentes armonizados de programa informático de un sistema HCE contendrá toda la información siguiente:

1. El nombre del sistema HCE, su versión y cualquier otra referencia que permita la identificación del sistema de forma inequívoca.
2. El nombre y la dirección del fabricante o, en su caso, de su representante autorizado.
3. Una indicación de que la declaración UE de conformidad se emite bajo la responsabilidad exclusiva del fabricante.
4. Una declaración de que el sistema HCE en cuestión es conforme con las disposiciones del capítulo III y, en su caso, con cualquier otro acto de Derecho de la Unión pertinente que disponga la emisión de una declaración UE de conformidad, complementada por los resultados obtenidos en el entorno de pruebas mencionado en el artículo 40.
5. Las referencias a las normas armonizadas pertinentes utilizadas, en relación con las cuales se declara la conformidad.
6. Las referencias a las especificaciones comunes utilizadas, en relación con las cuales se declara la conformidad.
7. El lugar y la fecha de emisión de la declaración, así como la firma, el nombre y el cargo de la persona que ha firmado y, en su caso, una indicación de la persona en cuyo nombre se ha firmado.
8. En su caso, información adicional.