

Recomendación del Consejo sobre  
Gobernanza de Datos de Salud

**Instrumentos Legales de la OCDE**

OCDE

Mejores políticas para una vida mejor

El presente documento se publica bajo la responsabilidad del Secretario General de la OCDE. Reproduce un Instrumento Legal de la OCDE y puede contener material adicional. Las opiniones expresadas y los argumentos empleados en el material adicional no reflejan necesariamente el parecer oficial de los países miembros de la OCDE.

Tanto este documento como cualquier dato y mapa que se incluyan en él no conllevan perjuicio alguno respecto al estatus o la soberanía de cualquier territorio, a la delimitación de fronteras y límites internacionales ni al nombre de cualquier territorio, ciudad o área.

A fin de acceder a los textos oficiales y actualizados de los instrumentos legales de la OCDE, así como a cualquier otra información relacionada, sírvase consultar el compendio de instrumentos legales de la OCDE en <http://legalinstruments.oecd.org>.

**Por favor, cite esta publicación de la siguiente manera:**

OECD, *Recommendation of the Council on Health Data Governance, (Recomendación del Consejo sobre gobernanza de datos de salud)*, OECD/LEGAL/0433

Serie: Instrumentos legales de la OCDE

© OCDE 2018

Este documento se proporciona de forma gratuita. Puede reproducirse y distribuirse gratuitamente sin necesidad de otros permisos, siempre y cuando no se modifique de ninguna manera. No puede ser vendido.

Este documento está disponible en los dos idiomas oficiales de la OCDE (inglés y francés). Puede ser traducido a otros idiomas, siempre y cuando se indique como “traducción no oficial” e incluya la siguiente exclusión de responsabilidad: *"Esta traducción ha sido realizada por [NOMBRE DEL AUTOR DE LA TRADUCCIÓN] solo con fines informativos y la OCDE no garantiza su precisión. Las únicas versiones oficiales son los textos en inglés y francés disponibles en el sitio web de la OCDE <http://legalinstruments.oecd.org>"*

*Esta traducción ha sido realizada por SILVANA DÍAZ ALVARADO solo con fines informativos y la OCDE no garantiza su precisión. Las únicas versiones oficiales son los textos en inglés y francés disponibles en el sitio web de la OCDE <http://legalinstruments.oecd.org>"*

**Fecha(s)**

Adoptado el 13/12/2016

**Antecedentes**

La Recomendación sobre gobernanza de datos de salud fue adoptada por el Consejo de la OCDE el 13 de diciembre de 2016 según la propuesta del Comité de Salud y del Comité de Políticas de la Economía Digital. Esta Recomendación reconoce que muchos miembros de la OCDE carecen de un marco coordinado de política pública que oriente el uso de datos de salud y las prácticas de intercambio en materia de salud con el fin de proteger la privacidad, permitir alcanzar altas cotas de eficiencia, promover la calidad y fomentar la investigación innovadora. Su objetivo principal es recomendar que los Adherentes establezcan e implementen un marco de gobernanza de datos de salud nacional para poner a disposición y usar los datos de salud personales con fines de interés público vinculados a la salud y promover la protección de la privacidad, los datos de salud personales y la seguridad de datos. La Recomendación tiene por objetivo brindar una mayor armonización entre los marcos de gobernanza de datos de salud de los Adherentes, de manera que más países se beneficien del uso de datos estadísticos y de investigación con fines de interés público y de esta manera, que más países puedan participar en proyectos estadísticos y de investigación multipaís, protegiendo a la vez la privacidad y la seguridad de datos.

## EL CONSEJO

**TENIENDO EN CUENTA** el literal b) del Artículo 5 del Convenio sobre la Organización para la Cooperación y el Desarrollo Económicos del 14 de diciembre de 1960;

**TENIENDO EN CUENTA** la Recomendación del Consejo relativa a las Directrices que Regulan la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales [C(80)58/FINAL, modificado por C(2013)79], la Recomendación del Consejo sobre biobancos humanos y bases de datos de investigación genética [C(2009)119] y la Recomendación del Consejo sobre la gestión de riesgos en seguridad digital para la prosperidad económica y social [C(2015)115];

**OBSERVANDO** el informe de la OCDE sobre *Health Data Governance: Privacy, Monitoring and Research* (Gobernanza de datos de salud: Privacidad, monitoreo e investigación (OECD, 2015);

**RECONOCIENDO** que el acceso y el procesamiento de datos personales de salud pueden servir para alcanzar los intereses públicos relacionados con la salud y aportar beneficios significativos a los individuos y a la sociedad;

**RECONOCIENDO** que los sistemas de salud se ven cada vez más afectados por un volumen creciente de datos personales de salud en formato electrónico, incluidos los registros electrónicos de salud y registros administrativos; que dichos datos son a menudo conservados en silos de datos por las organizaciones que los han recopilado y por las autoridades gubernamentales, tales como ministerios de salud y agencias estadísticas; y que cuando ocurra la transferencia segura, la interconexión y el análisis de los datos de salud, el valor de los datos con fines de interés público relacionados con la salud aumentará significativamente.

**RECONOCIENDO** que se debe mantener la confianza pública en la protección de los datos personales de salud si se logran los beneficios que se pueden obtener a través de su procesamiento; y que los gobiernos tienen la función de impulsar el cumplimiento de las leyes y políticas de privacidad.

**RECONOCIENDO** que los datos personales de salud, por su naturaleza delicada y según las normas éticas y el principio del secreto médico, requieren un nivel de protección especialmente elevado, y que los avances tecnológicos pueden permitir tanto la protección de datos personales de salud así como también pueden introducir nuevos riesgos para la privacidad y la seguridad de los datos;

**RECONOCIENDO** que el logro de estos beneficios requiere el cuidadoso desarrollo y la aplicación de sólidos marcos de gobernanza de datos de salud, apropiados para el contexto y capaces de proteger la privacidad y que estos requieren a su vez que se identifiquen y se gestionen los riesgos en materia de privacidad y seguridad;

**RECONOCIENDO** que, aunque los Miembros y no Miembros que se adhieren a la presente Recomendación (en adelante, los "Adherentes") están invirtiendo en la infraestructura de datos de salud y que se han realizado considerables progresos en este sentido para lograr marcos coordinados de gobernanza de los datos de salud, se deben abordar numerosas diferencias en cuanto a la disponibilidad, el acceso y el uso de datos personales de salud, tanto dentro como fuera de las fronteras nacionales; y

**CONSIDERANDO** que, si bien existen diferencias en sus legislaciones nacionales, la protección efectiva del interés público es una función importante de los gobiernos; que la gobernanza de datos

de salud no es solo de competencia de los gobiernos centrales, sino que abarca todos los niveles de gobierno en los que se aplican diferentes mandatos en diferentes países; y que, por consiguiente, esta Recomendación es pertinente para todos los niveles del gobierno.

**Con relación a la propuesta del Comité de Salud y del Comité de Políticas de la Economía Digital:**

I. **ACUERDA** que la presente Recomendación se aplica al acceso y al procesamiento de los datos personales de salud para fines de interés público relacionados con la salud, tales como mejorar la calidad, la seguridad y la capacidad de respuesta de la atención de salud; reducir los riesgos de salud pública; descubrir y evaluar nuevas herramientas de diagnóstico y tratamientos para mejorar los resultados de salud; gestionar los recursos de atención de salud de manera eficiente; contribuir al progreso de la ciencia y la medicina; mejorar la planificación y evaluación de las políticas públicas; y mejorar la participación y las experiencias de los pacientes en la atención sanitaria.

II. **ACUERDA** que, a efectos de la presente Recomendación, los siguientes términos técnicos requieren una breve descripción para respaldar un entendimiento común:

- "Datos personales de salud" se refiere a cualquier información relativa a una persona identificada o identificable, que está relacionada con su salud y que incluye cualquier otro dato personal asociado.

- "Procesamiento de datos personales de la salud" se refiere a todas las operaciones relacionadas con datos y que involucran datos personales de salud como la recopilación, el uso, la divulgación, el almacenamiento, el registro, la edición, la recuperación, la transferencia, el intercambio, la interconexión o combinación, el análisis y eliminación de datos.

- "Anonimización" se refiere al proceso por el cual se altera un conjunto de datos personales de salud, de manera que la información resultante no pueda ser fácilmente asociada con personas en particular. Los datos anonimizados no son datos anónimos. La "reidentificación" se refiere al proceso por el cual la información es atribuida a los datos anonimizados para identificar a la persona a la que se relacionan los datos anonimizados.

III. **RECOMIENDA** que los gobiernos establezcan e implementen un marco nacional de gobernanza de datos de salud a fin de fomentar la disponibilidad y uso de datos personales de salud para fines de interés público relacionados con la salud, promoviendo a su vez la protección de la privacidad, los datos personales de salud y la seguridad de los datos. Dicho marco de gobernanza de datos de salud debería contemplar:

**1. Compromiso y participación**, especialmente a través de consultas públicas, de una amplia gama de interesados con el fin de garantizar que el procesamiento de datos personales de salud en este contexto sirva al interés público y sea consistente con los valores de la sociedad y las expectativas razonables de los individuos tanto para la protección de sus datos como para el uso de sus datos destinados a la gestión del sistema de salud, investigación, estadísticas u otros fines relacionados con la salud que sirvan al interés público.

**2. Coordinación en el ámbito del gobierno y promoción de la cooperación entre organizaciones de procesamiento de datos personales de salud, tanto en el sector público como en el privado.** Esta cooperación debería:

i. fomentar elementos y formatos de datos comunes; promover la garantía de calidad e impulsar las normas de interoperabilidad de datos; y

ii. fomentar políticas y procedimientos comunes que reduzcan al mínimo las barreras para el intercambio de datos en materia de gestión del sistema de salud, estadísticas, investigación y otros fines de interés público relacionados con la salud, protegiendo al mismo tiempo la privacidad y la seguridad de los datos.

**3. Revisión de la capacidad de los sistemas de datos de salud del sector público empleados para procesar datos personales de salud que sirvan y protejan el interés público.** Dicha revisión debería incluir:

i. Disponibilidad de datos, calidad, idoneidad para el uso, accesibilidad, así como protección de privacidad y seguridad de datos.

ii. Elementos del procesamiento de datos que están permitidos para la gestión del sistema de salud, investigación, estadísticas u otros fines de interés público relacionados con la salud, en función de las garantías adecuadas, en particular transferencias de una serie de datos e interconexión de los registros de dichos datos.

**4. Disposición de la información de manera clara para las personas.** Al poner dicha información a disposición, se debería garantizar que:

i. cuando se recaben datos personales de salud de la gente, la información sobre el procesamiento de sus datos personales de salud, incluido un posible acceso lícito por terceros, los objetivos subyacentes de dicho procesamiento y sus beneficios así como su base legal sean difundidos de forma clara, precisa, evidente y fácil de entender;

ii. las personas sean notificadas de manera oportuna sobre cualquier violación importante de datos personales u otro mal uso de sus datos personales de salud. Cuando no se pueda hacer notificaciones de manera individual, la notificación será realizada mediante comunicación pública eficaz.

**5. Consentimiento informado y alternativas adecuadas**

i. Los mecanismos de consentimiento deberían:

a. proporcionar claridad a fin de saber si se requiere el consentimiento individual para el procesamiento de sus datos personales de salud y, de ser así, los criterios utilizados para hacer esta determinación; establecer lo que constituye un consentimiento válido y cómo se puede retirar el consentimiento; y las alternativas y exenciones legales a la exigencia del consentimiento, incluso las circunstancias excepcionales en las que la obtención del consentimiento es imposible, impracticable o incompatible con la consecución del objetivo de interés público relacionado con la salud y el procesamiento está sujeto a garantías compatibles con la presente Recomendación;

b. disponer que, cuando el procesamiento de datos personales de salud se base en el consentimiento, dicho consentimiento sólo debería ser válido si es informado y otorgado libremente y si es que se les otorga a las personas mecanismos claros, evidentes y fáciles de usar a fin de proporcionar o retirar el consentimiento para el uso futuro de los datos.

ii. Cuando el procesamiento de datos personales sobre la salud no se base en el consentimiento, los mecanismos deberían estipular, en la medida de lo posible, que:

a. las personas puedan expresar sus preferencias con respecto al procesamiento de sus datos personales de salud, lo que incluirá no sólo la posibilidad de oponerse al procesamiento bajo ciertas circunstancias sino también la habilidad de solicitar activamente que se compartan sus datos personales de salud para investigación u otros fines de interés público relacionados con la salud;

b. si las objeciones o solicitudes de procesamiento de datos no pueden ser atendidas, entonces se debe proporcionar a las personas las razones correspondientes, lo que incluirá la base jurídica pertinente.

**6. Procedimientos de revisión y aprobación, según corresponda, sobre el uso de datos personales de salud con fines de investigación y otros propósitos de interés público relacionados con la salud.** Dichos procedimientos de revisión y aprobación deberían:

i. implicar una evaluación basada en la evidencia para determinar si el uso propuesto es de interés público;

ii. ser sólidos, objetivos y justos;

iii. operar de manera que sea oportuna y que promueva la consistencia de los resultados;

iv. operar con transparencia, protegiendo al mismo tiempo los intereses legítimos; y

v. estar respaldados por una revisión independiente y multidisciplinaria realizada por aquellos con la experiencia necesaria para evaluar los beneficios y los riesgos del procesamiento y la mitigación de riesgos para las personas y la sociedad.

**7. Transparencia, a través de mecanismos de información pública que no comprometan la privacidad de los datos de salud, la protección de seguridad, los intereses comerciales legítimos ni otros intereses de las organizaciones.** La información pública debería incluir los siguientes elementos:

i. Los propósitos del procesamiento de los datos personales de salud y los fines de interés público vinculados a la salud, así como su fundamento jurídico.

ii. El procedimiento y los criterios empleados para aprobar el procesamiento de los datos personales de salud y un resumen de las decisiones de aprobación adoptadas, incluida una lista de las categorías de los destinatarios de datos aprobados.

iii. Información sobre la implementación del marco de gobernanza de datos de salud y su efectividad.

**8. Maximización del potencial y promoción del desarrollo de la tecnología** como medio de permitir la disponibilidad, la reutilización y el análisis de los datos personales de salud, protegiendo, al mismo tiempo, la privacidad y la seguridad y facilitando a las personas el control del uso de su propia información.

**9. Mecanismos de seguimiento y evaluación.** Estos mecanismos deberían:

i. evaluar si los usos de los datos personales de salud han cumplido con los objetivos de interés público previstos relacionados con la salud, si se produjeron los beneficios que se esperaba de tales usos y si tales uso tuvieron consecuencias negativas, incluidos los casos en los que no se haya podido cumplir con los requerimientos nacionales para la protección de la privacidad, de los datos personales de salud y la seguridad de los datos; casos en los que haya habido violación de datos y usos indebidos de datos. Asimismo, estos mecanismos deberían incorporar los resultados de dicha evaluación en un proceso de mejora continua, incluso a través de:

a. una revisión periódica de la evolución de la disponibilidad de datos personales de salud, las necesidades de investigación en salud y actividades relacionadas, y las necesidades de políticas públicas; y

b. una evaluación y actualización periódica de las políticas y prácticas de gestión de la privacidad, la protección de los datos personales de salud y los riesgos para la seguridad en relación con la gobernanza de los datos personales de salud.

ii. alentar a quienes procesan datos personales de salud a que revisen y evalúen periódicamente la capacidad, la fiabilidad y la vulnerabilidad de las tecnologías empleadas.

**10. Establecimiento de una capacitación adecuada y desarrollo de competencias en medidas de privacidad y seguridad para quienes procesan datos personales de salud**, que estén en consonancia con las normas vigentes y normas técnicas de procesamiento de datos.

**11. Implementación de controles y garantías.** Estos deberían:

i. proporcionar cadenas de responsabilidad claras y estables para el procesamiento de datos personales de salud, acompañadas de mecanismos adecuados de auditoría;

ii. establecer requisitos para que los datos personales de salud sólo puedan ser procesados o sean responsabilidad de las organizaciones con una formación adecuada de todos sus funcionarios en materia de privacidad y seguridad de datos,

en consonancia con sus funciones y responsabilidades relativas al procesamiento de datos personales de salud y según cualquier código de conducta profesional aplicable;

iii. animar a las organizaciones que procesan datos personales de salud a designar a un empleado o empleados para que coordine(n) y sea(n) responsable(s) del programa de seguridad de la información de la organización, lo que incluirá informar a la organización y a sus empleados sobre sus obligaciones legales para proteger la privacidad y la seguridad de los datos;

iv. incluir procesos formales de gestión de riesgos, actualizados periódicamente, que evalúen y procesen los riesgos, así como la eliminación involuntaria de datos, la reidentificación, las infracciones u otros usos indebidos, en particular cuando se establecen nuevos programas o se introducen prácticas novedosas;

v. incluir medidas tecnológicas, físicas y organizativas destinadas a proteger la privacidad y la seguridad, manteniendo al mismo tiempo, en la medida de lo posible, la utilidad de los datos personales de salud para fines de interés público relacionados con la salud. Tales medidas deberían incluir:

a. mecanismos que limiten la identificación de las personas, incluso a través de la anonimización de sus datos personales de salud y tomen en consideración el uso propuesto de los datos, permitiendo al mismo tiempo la reidentificación cuando sea aprobada. La reidentificación puede ser aprobada para llevar a cabo futuros análisis de datos para la gestión del sistema de salud, investigación, estadísticas u otros aspectos de interés público relacionados con la salud; o para informar a una persona sobre una afección específica o resultado de la investigación, cuando proceda;

b. acuerdos al compartir datos personales de salud con terceros para fines de procesamiento que ayuden a maximizar los beneficios y gestionar los riesgos, preservando al mismo tiempo la utilidad de los datos personales de salud. Dichos acuerdos deberían especificar disposiciones para la transferencia segura de datos e incluir medios adecuados para sancionar eficazmente el incumplimiento;

c. cuando sea factible y apropiado, examinar alternativas para la transferencia de datos a terceros, como centros de acceso seguro a los datos e instalaciones de acceso remoto a los datos;

d. una buena verificación de identidad y autenticación de las personas que acceden a los datos personales de salud.

**12. Exigencia a las organizaciones que procesan datos personales de salud para que demuestren su cumplimiento con las expectativas nacionales en cuanto a la gobernanza de los datos de salud.** Para este propósito se podría establecer una certificación o acreditación para las organizaciones de procesamiento de datos personales de salud, en la medida en que estas certificaciones o acreditaciones ayuden a implementar normas para el procesamiento

de datos personales de salud o a demostrar la capacidad de cumplir con las normas reconocidas de gobernanza.

**IV. RECOMIENDA** que los gobiernos apoyen la cooperación transfronteriza en la tramitación de datos personales de salud para la gestión del sistema de salud, investigación, estadísticas y otros fines relacionados con la salud que sirvan al interés público, en función de las garantías acordes con la presente Recomendación. Para dicho efecto, los gobiernos deberían:

- i. identificar y eliminar los obstáculos para una cooperación transfronteriza efectiva en el procesamiento de los datos personales de salud con fines de interés público relacionados con la salud, de manera adecuada para proteger la privacidad y la seguridad de los datos, a la luz de todas las circunstancias;
- ii. facilitar la compatibilidad o la interoperabilidad de los marcos de gobernanza de datos de salud;
- iii. promover la mejora continua a través del intercambio de resultados y mejores prácticas al disponer y emplear los datos personales de salud para la gestión del sistema de salud, la investigación, las estadísticas y otros propósitos relacionados con la salud en beneficio del interés público.

**V. RECOMIENDA** que los gobiernos colaboren con los expertos y organizaciones pertinentes para desarrollar mecanismos que sean coherentes con los principios de la presente Recomendación y que permitan el intercambio eficiente y la interoperabilidad de los datos de salud, protegiendo al mismo tiempo la privacidad, y cuando sea pertinente, los códigos, las normas y la estandarización de la terminología de los datos de salud.

**VI. ALIENTA** a las organizaciones no gubernamentales a que sigan la presente Recomendación cuando procesen datos personales de salud para fines relacionados con la salud en beneficio del interés público.

**VII. INVITA** al Secretario General a que difunda esta Recomendación.

**VIII. INVITA** a los Adherentes a que difundan esta Recomendación en todos los niveles de gobierno.

**IX. INVITA** a los No Adherentes a que tengan en cuenta esta Recomendación y se adhieran a ella.

**X. ENCARGA** al Comité de Salud, en cooperación con el Comité de Políticas de la Economía Digital a que:

- a) sirva de foro para el intercambio de información sobre avances y experiencias en relación con la implementación de la presente Recomendación, y;
- b) supervise la implementación de la presente Recomendación e informe sobre su adopción al Consejo en un plazo de cinco años y posteriormente a esa fecha, según corresponda.