Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas
Año VII. Vol. VII. N° 1. Edición Especial. 2022
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela

http://dx.doi.org/10.35381/racji.v7i1.2203

Protección de datos personales en la historia clínica electrónica bajo el marco legal ecuatoriano

Protection of personal data in the electronic medical record under the Ecuadorian legal framework

Jefferson Norberto Martínez-Jara
jefferson.martinez.72@est.ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Cuenca
Ecuador
https://orcid.org/0000-0003-1531-9463

Juan Carlos Pérez-Ycaza
juan.perezy@ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Cuenca
Ecuador
https://orcid.org/0000-0003-1569-1898

Recibido: 15 de agosto 2022
Revisado: 01 de octubre 2022
Aprobado: 15 de noviembre 2022
Publicado: 01 de diciembre 2022

Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas
Año VII. Vol. VII. N° 1. Edición Especial. 2022
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela

RESUMEN

La constante evolución de las tecnologías de la información y de la comunicación ha permitido gestionar y almacenar datos personales de los usuarios de las instituciones prestadoras de servicios sanitarios. Se tiene por objetivo analizar el nivel de cumplimiento de la nueva Ley Orgánica de la Protección de Datos Personales en lo que respecta a los datos relativos a la salud en un integrante de los subsistemas de salud ecuatoriano. La investigación tiene enfoque cualitativo, para el análisis se utiliza la información que se ha recopilado sobre la historia clínica electrónica del desarrollador, se establece el cumplimiento de las garantías legales de los usuarios a la protección de sus datos personales según el marco jurídico vigente; con los resultados, se proponen mecanismos de acción para que este derecho se garantice.

Descriptores: Derecho a la privacidad; protección de datos; legislación de las comunicaciones. (Tesauro UNESCO).

ABSTRACT

The constant evolution of information and communication technologies has made it possible to manage and store personal data of the users of the institutions providing health services. The objective is to analyze the level of compliance with the new Organic Law for the Protection of Personal Data regarding health-related data in a member of the Ecuadorian health subsystems. The research has a qualitative approach, for the analysis the information that has been collected on the developer's electronic health record is used, the compliance with the legal guarantees of the users to the protection of their personal data according to the current legal framework is established; with the results, mechanisms of action are proposed so that this right is guaranteed.

Descriptors: Right to privacy; data protection; communication legislation. (UNESCO Thesaurus).

INTRODUCCION

En la actualidad, debido al notable desarrollo de las tecnologías de la información y la comunicación, los usuarios informáticos pueden acceder a datos de diversa índole, en cualquier lugar y tiempo; y, dependiendo de su tipología, es posible encontrar información educativa, social, tecnológica, inclusive, en determinadas ocasiones, es factible obtener datos sensibles de las personas naturales y jurídicas.

Este desarrollo tecnológico ha sido aprovechado y aplicado en establecimientos que prestan servicios de salud para almacenar y procesar datos de los pacientes que acuden a estos centros sanitarios. La informática para gestionar datos de la salud es muy diversa, abarca una variedad de tecnologías, desde la visualización de simples gráficos hasta la toma de decisiones más compleja y la integración con la tecnología médica a través de los múltiples equipos y la interoperabilidad de redes.

La tecnología de la información de atención médica ofrece muchas oportunidades para mejorar y transformar la atención médica al reducir el error humano, mejorar los resultados clínicos, facilitar la coordinación de la atención, mejorar la eficiencia de la práctica y rastrear datos a lo largo del tiempo (Alotaibi & Frank , 2017). En este contexto, las instituciones sanitarias deben disponer de políticas de protección de sus datos informáticos, con el propósito de que usuarios no autorizados no puedan obtener datos de salud del paciente, para ello, se deben diseñar y documentar los mecanismos administrativos, técnicos y legales que garanticen el derecho a la protección de estos datos personales.

Bajo esta premisa, en el 2021 la Asamblea Nacional del Ecuador, para precautelar los datos personales de los ciudadanos, ha expedido la Ley Orgánica de Protección de Datos Personales (en adelante, LOPDP), la cual, es un instrumento jurídico que busca proteger la información de los datos personales. El capítulo IV de la LOPDP versa sobre las categorías especiales de los datos, entre ellos los datos relativos a la salud (Ley Orgánica de Protección de Datos Personales, 2021, p. 18).

En el Sistema Nacional de Salud ecuatoriano se encuentran inmersas las diferentes instituciones públicas y privadas que proporcionan servicios de prestación de servicios sanitarios, las cuales se sujetarán a las disposiciones de la Ley Orgánica de Salud,

según lo establecido en el artículo 2 de dicha Ley (Ley Orgánica de Salud, 2006); en muchas de ellas, para gestionar sus actividades han desarrollado sistemas informáticos, y, a partir de ello se establecen las siguientes preguntas: ¿Qué tan confiables son los sistemas de información que contienen datos de salud de los pacientes?, ¿existe normativa que especifica el acceso seguro a la historia clínica electrónica de los pacientes?, ¿es cuestionable la seguridad de los sistemas informáticos que contienen datos de la historia clínica electrónica?, ¿la normativa vigente en materia de gestión cumple con las disposiciones de la LOPDP?

Debido a estas interrogantes es necesario determinar el nivel de la protección de los datos personales en la historia clínica electrónica (en adelante, HCE) y el cumplimiento de los artículos 30, 31 y 32 de la LOPDP respecto a los datos relativos de salud en la HCE; asimismo, se busca identificar los mecanismos de protección que se han instaurado para precautelar los datos, y determinar si los procedimientos administrativos establecidos para el acceso a los sistemas informáticos cumplen con lo normado con relación a la protección de datos personales.

La regulación de los métodos y herramientas de protección de datos tiene por objeto garantizar la integridad de su uso de conformidad con la protección de los derechos de los titulares de esta información, y, en el mismo sentido, evitar afectar a los usuarios que operan los sistemas de información. Como consecuencia de una inapropiada custodia de los datos personales en la HCE, se generan un sinnúmero de problemas, entre algunos de ellos la vulneración de derechos y sus consecuencias jurídicas, la desconfianza en los sistemas de información electrónica por falta de privacidad y violación al derecho de la intimidad, entre otros.

Por lo expuesto, es importante que las instituciones de salud actualicen sus protocolos y procedimientos administrativos y tecnológicos, enmarcados en las normas internacionales de ciberseguridad, para disminuir las brechas de seguridad que actualmente se suscitan bajo el nuevo marco jurídico.

Se tiene por objetivo analizar el nivel de cumplimiento de la nueva Ley Orgánica de la Protección de Datos Personales en lo que respecta a los datos relativos a la salud en un integrante de los subsistemas de salud ecuatoriano.

MÉTODO

La presente investigación tiene carácter descriptivo documental con diseño bibliográfico, utilizando inicialmente documentación pública emitida por la Contraloría General del Estado, que se encuentra disponible en su portal web; asimismo, como otro recurso se empleó la información personal de la Historia Clínica Electrónica del desarrollador de la investigación.

Lo que se requiere analizar cómo se ha implementado la seguridad de los datos personales en relación con la Ley de control y lo que se regula en materia de protección de datos personales. Entre las hipótesis presentadas en la investigación se encuentra que la protección de los datos personales relacionados con la salud no es suficiente en el sentido de la LOPDP.

ANÁLISIS DE LOS RESULTADOS

Se tiene el proceso analítico de la información escrutada:

Historia Clínica (HC)

En las instituciones sanitarias se registran los servicios que se proporcionan a los usuarios por medio de documentos que contienen información, valoraciones y todo tipo de datos sobre el estado y evolución clínica del paciente durante el tratamiento o el proceso asistencial, por tanto, se define a la historia clínica como toda esta documentación escrita y gráfica de la salud y la enfermedad de un individuo y las acciones sanitarias resultantes de esos episodios (Amézqueta-Goñi et al., 2003, p. 24). Con el descubrimiento de nuevos instrumentos de escaneo y la llegada de pruebas adicionales como son las de laboratorio, imágenes diagnósticas y otras, estos documentos se anexan a los registros clínicos como parte del historial del paciente, es decir, en su historia clínica (Siegler, 2010, p. 671)**.**

Indistintamente de quién sea la persona que realice la prestación del servicio, el lugar o el área en dónde se proporcione la atención sanitaria, los documentos son registrados y almacenados en conjunto en la historia clínica de los pacientes.

Para actualizar la administración de la Historia Clínica Única, el Ministerio de Salud Pública del Ecuador, a través del Registro Oficial No. 378 de 26 de enero de 2021, publicó el Acuerdo Ministerial No. 00115-2021 suscrito el 10 de enero de 2021, el cual expide el Reglamento para el manejo de la Historia Clínica Única. Posteriormente, en el Cuarto Suplemento del Registro Oficial No. 454 de 18 de mayo de 2021, se presenta la Fe de errata, en el que se publicaron los anexos que no fueron presentados inicialmente (Reglamento para el manejo de la historia Clínica Única, 2021).

En el artículo 3 del mencionado Reglamento se establecen las definiciones de dos tipos de historias clínicas, la tradicional denominada Historia clínica física, y la nueva en formato electrónico llamada Historia clínica electrónica. La primera hace referencia como un documento que se encuentra en formato físico; esta dispone de información confidencial y veraz del usuario o paciente, que es generado obligatoriamente por el personal de salud en cada uno de los procesos asistenciales, es decir, en cada una de las atenciones brindadas, en forma sistemática con los datos obtenidos de las atenciones, de los diagnósticos obtenidos y sus respectivos tratamientos (Reglamento para el manejo de la historia Clínica Única, 2021, p. 6). Esta normativa establece que, antes de empezar las atenciones de salud en los usuarios o pacientes, la historia clínica, sea cual fuese su naturaleza, física o electrónica, es de apertura obligatoria, y que los datos rigen por el principio de confidencialidad, obligando de esta manera a que el personal sanitario al que tenga acceso a esta información debe guardar el sigilo correspondiente.

Historia Clínica Electrónica (HCE)

El desarrollo tecnológico ha permitido que las organizaciones contemplen la inclusión en sus sistemas de gestión sanitarios, tal es el caso que la Organización Mundial de la Salud, en la edición Nro. 58 de la asamblea mundial de la salud, reconocía que se debe facilitar integrar la cibersalud en los sistemas de servicios de salud, en telemedicina, y en la profesionalización de los servidores sanitarios, con el objetivo de mejorar el acceso, calidad y seguridad de la atención sanitaria (World Health Organization, 2005, p. 110).

Estos acontecimientos han generado que las instituciones que prestan los servicios de salud se orienten en desarrollar sus sistemas informáticos para migrar hacia un nuevo enfoque, de la historia clínica tradicional física a la nueva historia clínica electrónica, debido a que, actualmente, mantener y gestionar documentos físicos en lugar de electrónicos es considerado un anacronismo.

Es claro que los beneficios de disponer de la HCE son muchos, entre los cuales podemos encontrar, acceso desde cualquier lugar y tiempo, información completa y disponible para varios usuarios de forma simultánea, soporte de la información por equipos multidisciplinarios, seguridad, interoperabilidad de las bases de datos de salud, análisis epidemiológicos y de investigación y docencia, confidencialidad, entre otros (Carnicero Giménez de Azcárate, 2003, p. 71).

Estos cambios en los paradigmas de registrar datos relativos a la salud perciben una gran importancia, debido a que, utilizar plataformas de diversos sistemas informáticos que se encuentran en perenne interacción con el internet, en constante riesgo de vulneración y acceso no permitido por parte de terceros, compromete los derechos de privacidad y confidencialidad de los usuarios o pacientes.

En el artículo 4 de La Ley Orgánica de Salud, establece que la autoridad sanitaria nacional es el Ministerio de Salud Pública, a quien corresponde la dirección de las tareas de atención de la salud, la aplicación, vigilancia y control de la citada Ley (Congreso Nacional del Ecuador, 2006), por ello, para garantizar y cumplir lo establecido en la Ley, ha establecido las directrices técnicas, administrativas y jurídicas en las cuales deben regirse las Historias Clínicas.

Por la importancia que tiene la HCE se han realizado varios análisis en la gestión de seguridad de la información, así es que, en el artículo 1 del Acuerdo ministerial 1190 del Ministerio de Salud Pública del Ecuador, publicado en el Registro Oficial 622 del 19 de enero del 2012, se aprobó que se puedan utilizar los estándares Health Level Seven (HL7), al mismo tiempo dispone que estos se implementen en todas las instituciones del Sistema Nacional (Acuerdo 1190); esto implica que deben emplear las normativas internacionales de informática en salud para el desarrollo del software asistencial sanitario, en los que incluyen datos de salud de usuarios o pacientes en

las historias clínicas que, por la naturaleza y estructura de la información son de carácter electrónico.

Posteriormente, mediante el Acuerdo 0009-2017 (Registro Oficial 968, 22-III-2017), el Ministerio de Salud (en adelante, MSP), instaura el Reglamento para el manejo de la historia clínica electrónica para que se pueda implementar la HCE (Reglamento para el Manejo de la Historia Clínica Electrónica, 2017), lo propio para definir las directrices de su aplicación en los establecimientos prestadores de servicios sanitarios, en todo el territorio nacional. En el artículo 3 de este Reglamento se conceptualiza a la HCE como un registro electrónico de carácter personal, que resulta de una atención de salud, encontrándose dispuesta y contenida en una base de datos, la cual es generada mediante programas informáticos y que se encuentra certificada con la firma electrónica del profesional de la salud que realizó la atención.

A continuación, el MSP, emite el Reglamento para el manejo de la historia clínica única, y define a la HCE como todo el conjunto integral de datos, sean estos clínicos, los sociales y económicos referidos a la salud de un individuo, desde su nacimiento hasta el final de sus días, los cuales se encuentran procesados a través de medios electrónicos, la cual es de igual valor y equivalencia funcionalmente a la tradicional historia clínica en papel (Reglamento para el manejo de la historia Clínica Única, p. 7).

El presente documento tiene por objeto regular el contenido de la historia clínica individual y los requisitos para su implementación por parte de los profesionales de la salud en las instituciones de salud del sistema nacional de salud. Con estas consideraciones, para cumplir con el Reglamento para el Manejo de la HCE, el MSP publica el Acuerdo No. 00089-2020 en el Segundo Suplemento del Registro Oficial No.348, del 11 de diciembre 2020, que versa sobre la Norma Técnica Historia Clínica Única Electrónica y Manual Historia Clínica Electrónica. Esta normativa dispone que debe ser aplicable de manera obligatoria para todos los integrantes del Sistema Nacional de Salud. Como parte de su objetivo general es garantizar la confidencialidad y seguridad de los registros electrónicos en salud (Norma Técnica Historia Clínica Única Electrónica y Manual Historia Clínica Electrónica, p. 7).

Interoperabilidad entre las entidades sanitarias

Para Indarte S. (Abad et al., 2012, p. 316) el desafío de las instituciones de salud es producir sistemas de datos informáticos que permitan tener una gestión eficaz, eficiente y centrada en el ciudadano. Una de las principales características de estos sistemas de información es la interoperabilidad, ya que permite que la comunicación pueda ser transversal y longitudinal dentro de las estructuras de salud, lo que asegura la confidencialidad e integridad de la información intercambiada y el acceso oportuno a la misma. Técnicamente, el concepto de interoperabilidad, según el Instituto de Ingenieros Eléctricos y Electrónicos, ha sido definida como la capacidad de dos o más sistemas o componentes para intercambiar información y utilizarla (IEEE Standard Glossary of Software Engineering Terminology, 1990, p. 42).

Lo que hoy se entiende por interoperabilidad, es que los sistemas de Historias Clínicas Electrónicas, con características heterogéneas, puedan ser capaces de transmitir datos, entenderse e integrarse sin la intervención humana (Etreros-Huerta y otros, 2009, p. 468). No es discutible que la necesidad de que los sistemas de información puedan comunicarse entre ellos, a pesar de que sus plataformas tecnológicas sean de diferente naturaleza, con el afán de procesar una información clara, oportuna, precisa que pueda garantizar la integridad, seguridad y confidencialidad de los datos de índole sanitario.

Sin lugar a duda, en pocos años, a nivel global, las organizaciones sanitarias desarrollarán sistemas de información y comunicación que permitirán disponer de la tan anhelada interoperabilidad, con características tan deseadas y desarrolladas que no solo podrán visualizar los datos clínicos y herramientas de diagnóstico, sino que también, a través de un complejo sistema de normas y protocolos de ciberseguridad se podrá garantizar la utópica confidencialidad y seguridad, derechos fundamentales de los ciudadanos.

Además, el desarrollo de la Inteligencia Artificial por medio de la generación de algoritmos matemáticos y lógicos permitirá obtener resultados de estudios clínicos, epidemiológicos, indicadores de gestión sanitarios, desarrollar la telemedicina en todas sus formas de una manera efectiva, interactuar estrechamente entre los

profesionales sanitarios o pacientes en tiempo real, emitir mensajes o señales de alerta a través de mensajes personalizados con los pacientes y otras acciones que potencialicen el desarrollo; siempre enmarcado en la normativa legal vigente y, sobre todo precautelando los derechos de las personas establecidos en la Constitución y los convenios internacionales.

En el marco de nuestra legislación, la característica de interoperabilidad de los sistemas informáticos que gestionan las HCE es tratada con suma importancia por la naturaleza de la misma; por consiguiente, el artículo 9 del Reglamento para el Manejo de la HCE, prescribe que esta se aplicará en el marco de la interoperabilidad, y se encuentra contemplada como la capacidad de los sistemas informáticos de los múltiples establecimientos de salud para interactuar entre ellos con similares; de tal forma se entiende que las diferentes instituciones sanitarias deben compartir la información con criterios similares de operación.

Con referencia a la firma electrónica inmersa en la interoperabilidad, se manifiesta que los sistemas informáticos de las HCE deben implementarlas como parte su gestión habitual para aprobar y reconocer el contenido de la HCE a través de esta certificación electrónica, debido a que, este nuevo tipo de firma, tiene los mismos efectos legales que una firma del tipo manuscrita, según lo establece la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en su artículo 14 (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002)

El concepto que el Reglamento para el manejo de la HCU proporciona sobre la HCE señala que la plataforma de interoperabilidad en salud tiene el objetivo de intercambiar la información clínica de los pacientes entre las diferentes instituciones privadas y públicas, con una infraestructura tecnológica y de diversos servicios que permitan obtener dicha conectividad. Esto hace alusión a que, las instituciones sanitarias, sean públicas y privadas, deben desarrollar sus plataformas informáticas bajo un mismo criterio, independientemente el software de desarrollo y seguridad informática, con el objetivo de intercambiar información sobre sus usuarios o pacientes, es decir, los datos relativos con la salud con su respectiva protección.

En el 2015, la Secretaría Nacional de la Administración Pública ha expedido la Norma Técnica de Interoperabilidad Gubernamental, que tiene como objetivo proporcionar las directrices y estándares técnicos para el transporte de los datos e información de naturaleza electrónica a las entidades que integran la Administración Pública Central Institucional y Dependiente de la Función Ejecutiva (APCID) por medio de la plataforma de Interoperabilidad de índole transversal (Norma Técnica de Interoperabilidad Gubernamental). El literal 11 del artículo 4.2 que versa sobre las obligaciones de las entidades de la APCID, manifiesta que dichas instituciones deben utilizar estándares como el HL7 (Health Level Seven), normas que son utilizadas en plataformas de datos sanitarios (American National Standards Institute (ANSI), 2022).

El derecho a la protección de los datos personales

Los pacientes proporcionan su información personal de salud a los profesionales sanitarios para que estos los analicen y puedan proporcionarles el servicio correspondiente y, de igual manera, en muchos casos tienen conocimiento que esta información es útil para que las instituciones provean otros tipos de servicios relacionados con sus prestaciones, como por ejemplo, los servicios de laboratorio, histopatología, farmacia, imagenología, historia laboral, seguros, estadística, entre otros.

Si bien es cierto, se conoce que esta información es registrada en sistemas informáticos, una gran mayoría de los usuarios no se percatan o no tienen el conocimiento suficiente sobre el nivel de protección de confidencialidad y seguridad que estos datos tienen, y cuán fácil es el acceso de terceros a dicha información; de la misma manera, desconocen si estos datos pueden ser utilizados en investigaciones no permitidas por los titulares o con fines comerciales desleales por parte de ciertas industrias farmacéuticas, pues el valor económico del tratamiento inescrupuloso de estos datos, permitidos o no, es alto y, por consiguiente, esta información ha llegado a ser en un bien permanente comercializado en los diferentes mercados como un aporte diario a los sistemas de información privados y gubernamentales (Remolina-Angarita, 2010, p. 5).

En este contexto, los datos personales, algunos muy sensibles como los relativos a la salud, desde hace algunos años han gozado de especial tratamiento por su connotación; es por ello que se ha proporcionado al derecho a la protección de los datos personales una importancia muy relevante, convirtiéndolo no solo en un derecho, sino en un derecho fundamental, concretamente en Europa, en dónde, presupone tanto su relación con otros derechos fundamentales como los principios constitucionales inevitablemente afectados por su existencia (Aguado-Renedo, 2010, p. 3).

El innegable desarrollo de las Tecnologías de la Información y de la Comunicación ha permitido sustancialmente la transmisión y accesibilidad de los datos, sin embargo, no se ha podido determinar la seguridad y confidencialidad en un entorno total, sino más bien, cada estado contempla algunos principios, deberes y derechos que se relacionan con el derecho a la protección de los datos personales, en la que destacan que al titular disponga su consentimiento para el tratamiento de su información con un objetivo en especial, excepto en condiciones particulares como en situaciones de emergencia médica (Gómez-Córdoba et al., 2020, p. 6).

Bajo esta óptica, partiendo de que el desarrollo tecnológico se incrementa incontrolablemente de forma permanente, y que para acceder a visualizar información privada y pública de los ciudadanos no es tan complicado e irrelevante como se presuponía, el derecho de la protección de los datos personales debe ser tratado con vital interés desde el ámbito jurídico, destacando normas y leyes que determinen los procedimientos para su tratamiento, inclusive establecer normas técnicas actualizables de acuerdo a la internacionalización de este tipo de protocolos.

La CRE garantiza los derechos de libertad, es por ello que en el numeral 19 del artículo 66 reconoce y garantiza a las personas su derecho a la protección de los datos carácter personal (Constitución de la República del Ecuador, 2008); de este modo, como una medida que garantice la protección de los datos personales, la Asamblea Nacional ha emitido la Ley Orgánica de Protección de Datos Personales publicada en el quinto Suplemento del Registro Oficial No.459 de 26 de mayo del 2021, en la cual dispone en su artículo 1 el objeto y finalidad de la misma, la cual garantiza el ejercicio

del derecho a la protección de datos personales, lo que incluye el acceso y resolución de datos de esta naturaleza y su correspondiente protección. Para ello, regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de protección (Ley Orgánica de Protección de Datos Personales, 2021).

En esa misma línea, en la LOPDP se encuentran establecidos los derechos a la información, normativa especializada de acceso, de eliminación, de rectificación y actualización de oposición, a la suspensión del tratamiento, a la portabilidad, a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, a la educación digital de consulta. Del mismo modo, se establecen algunas categorías especiales de datos, aquí se establecen los datos sensibles, los de niñas, niños y adolescentes, de salud y de las personas con discapacidad y de sus sustitutos, relativos a la discapacidad. En la presente investigación, se consideran los datos de la salud que se encuentran descritos en los artículos 31, 31 y 32 de la LOPDP.

Los datos relativos a la salud y su tratamiento

Los artículos 30, 31 y 32 de la LOPDP, determinan exclusivamente sobre los datos relativos de la salud; se reconoce que las instituciones que integran el Sistema Nacional de Salud y los profesionales sanitarios pueden ser partícipes de la adquisición y tratamiento de este tipo de datos relativos de salud o de los pacientes que estuvieron o que actualmente se encuentran bajo su tratamiento.

Este planteamiento, desde la óptica jurídica, trae consigo algunas dificultades interpretativas; por ejemplo, bajo esta perspectiva, no se especifican como se deben tratar los datos de pacientes que fueron atendidos en dichas instituciones o profesionales sanitarios anteriormente a la vigencia de la Ley, tampoco se menciona en esta era del conocimiento el tratamiento de los datos y su correlación con las historias clínicas electrónicas que deben mantener las instituciones sanitarias, sean públicas o privadas; no existe dinamismo en precisar las acciones que debe efectuar la autoridad sanitaria nacional frente a esta regulación.

Al mismo tiempo, en la normativa se resalta que los responsables y personas encargadas del tratamiento de los datos, y de todas las personas que intervengan en cualquier fase, deben mantener la confidencialidad para que existan la garantías de la seguridad de dichos datos personales. La relevancia con la que se promulga el principio de confidencialidad es importante, porque se enfatiza que por medio de él se posibilita garantizar la tan anhelada seguridad de estos datos con el objetivo de impedir la utilización inapropiada o ilícita de los mismos, al mismo tiempo evitar la pérdida, destrucción o daño alguno, sin embargo, paradógicamente, la previsión legal exceptúa el manejo tecnológico con el que se los debe gestionar.

A su vez, el principio de seguridad, establecido el literal j del artículo 10 de la LOPDP, establece que los responsables y personas encargadas de manejar los datos personales tienen que implementar las respectivas medidas de seguridad para proteger los datos; entre estas medidas podemos colegir las distintas normas técnicas informáticas de seguridad como la destacada norma ISO/IEC 27001:2013, que define los requisitos para poder crear, implementar, proporcionar mantenimiento y establecer mejora continua del sistema de gestión de seguridad de la información en la organización. También incluye evaluación de los riesgos de la seguridad de la información y los requisitos para el procesamiento adaptados a los requerimientos de cualquier organización (International Organization for Standardization, 2013).

Las consecuencias de la adopción de normas técnicas de seguridad son la protección y minimización sustancialmente de los riesgos, amenazas y vulnerabilidades que los datos personales puedan tener frente a potenciales irrupciones malintencionadas de terceros; este enfoque organizativo tiene por objeto establecer las bases para desarrollar planes de seguridad con el afán de mantener la confidencialidad y cumplir con el principio establecido en la LOPDP.

Es importante destacar que las medidas establecidas son complementarias al secreto profesional, estatuidas por los principios bioéticos, para que el programador o la inteligencia artificial, puedan aplicar filtros iniciales, durante el proceso y al final del sistema, como advertencias si la desviación tiene implicaciones bioéticas (García-Vigil, 2021, p. 298); igualmente, la norma establece que las obligaciones citadas

permanecen aun cuando las relaciones presentes entre el obligado o el encargado del proceso hayan terminado; esta obligatoriedad se infiere para que en lo posterior, a pesar de no existir un tratamiento presente, los datos personales guarden el respectivo sigilo, debido a que son perpetuos.

De la misma manera, está instaurada la disposición de no requerir el consentimiento del titular para que se produzca el tratamiento de los datos de salud por condiciones de interés público esencial en el área de salud, no obstante, es importante analizarla con una amplia reflexión ética para que sean sustentables, pues deben ser comunicadas en el momento de tomar decisiones para evitar perjuicios a los grupos en situación vulnerable, pérdida de confianza social y la necesaria coordinación entre actores principales (Esquivel-Guadarrama, 2020, p. 169).

Cabe destacar que es fundamental determinar el bien jurídicamente protegido de los titulares, como son la libertad y el libre desarrollo de todo proyecto esencial para su vida, y, por tanto, son más amplios que los bienes protegidos por la protección de los datos personales (Buisán i Espeleta, 2016, p. 5); no se debe especular suscitamente o colocar en una escala de prelación sin mayor análisis cuáles son los derechos y libertades más cruciales sin generar los mecanismos idóneos para protegerlos.

El artículo 31 de la LOPDP versa sobre el tratamiento de datos sobre salud, se establecen parámetros mínimos de cumplimiento para que puedan ser gestionados; entre ellos se encuentran que, los datos generados por los prestadores de servicios sanitarios, privados o públicos, deben aplicar los principios de confidencialidad y secreto profesional, tal como lo prescribre el artículo 326 de la Constitución vigente; asimismo, los titulares de los datos deben proporcionar su expreso consentimiento con el objetivo de tratar los datos, exceptuando en los casos en los que se requiere proteger intereses del interesado si tiene una discapacidad que le impida.

En similares circunstancias, cuando sean situaciones aplicables a medicina preventiva, capacidad laboral, diagnósticos médicos, prestaciones de varios servicios sanitarios o sociales, o gestión de los sistemas sanitarios o por medio de una relación contractual con un profesional sanitario el que debe está sujeto al secreto profesional.

A fin de que se pueda eliminar elementos para identificación inmediata de los pacientes, se ha establecido que, en lo posible, los datos deben ser previamente anonimizados o seudonimizados, como resultado del cumplimiento de estrictos requisitos éticos y legales en materia de confidencialidad y consentimiento (Amézqueta Goñi et al., 2003, p. 29); al mismo tiempo, este proceso deberá ser aprobado por la autoridad de protección de datos personales si se presenta un protocolo técnico que asegure este proceso.

A pesar de ello, con relación a este tema, surge la controversia sobre la anonimización, debido a que en la actualidad, en las sociedades globalmente informatizadas y automatizadas, con el auge de las tecnologías Big-data en Salud, las cuales procesan datos personales a gran escala, también se ha orientado a comercializarlos en el mismo sentido siendo un rentable modelo de negocio, y, anonimizados o seudonimizados no se supone que garantiza la protección de los datos, al contario puede constituir una suposición arriesgada, imprudente y potencialmente perversa basada en la sofisticación de la tecnología informática para hackear y manipular el acceso a conjuntos de datos o sistemas sanitarios (Observatorio de Bioética y Derecho, 2015, p. 2).

En relación con el artículo 32 de la LOPDP, se establece que la información de salud contenida en las instituciones del sistema de salud puede ser manipulada por terceros, personas naturales o jurídicas, privadas o públicas, con el objeto de realizar investigaciones científicas, si han sido anonimizadas o autorizadas por la autoridad de protección de datos personales.

Informe de Contraloría General del Estado - DNAI-AI-0050-2017

La Controlaría General del Estado realizó un proceso de examinación sobre la confidencialidad de la plataforma informática, para lo cual emitió un informe de auditoria interna con estos resultados (Contraloría General del Estado, 2017):

1. No se establecieron procedimientos para la administración de usuarios, configuración de seguridad y parametrización del Sistema de Información Médica.

2. No se establecieron procedimientos para el otorgamiento de una Identificación única a los usuarios del Sistema de Información Médica.
3. Cuentas de usuario del personal desvinculado de la Institución, se mantuvieron activas en el Sistema de Información Médica.
4. Acceso irrestricto a la información del Sistema sin acuerdos de confidencialidad suscritos.
5. Falta de formalización de procedimientos para acceso de usuarios.
6. Pistas de auditoría generadas para el Sistema, no permiten identificar el equipo desde el cual se generó la transacción.

Información de la Historia Clínica Electrónica

Actualmente, la institución objeto del análisis, ha emitido la siguiente información en respuesta a la solicitud de los datos de la HCE del investigador:

1. La información de datos de la HCE debe ser solicitada a la Casa de Salud, donde recibió la atención médica y de donde necesita su historial específicamente, ya que son los únicos que cuentan con los datos que el usuario requiere.
2. Los datos en el sistema informático datan aproximadamente del año 2015, por lo que no se encuentran registros anteriores a la fecha mencionada.
3. Evidencias de los registros encontrados en archivos de auditoría de la base de datos del sistema referente a: la fecha y hora de creación de la HCE en el sistema informático, nombre del usuario que creó la HCE, nombres de los usuarios que han accedido y editado la HCE con la evidencia respectiva, se indica además el nombre del software donde reposan los datos de HCE y que este se encuentra alojado en otra casa de salud diferente en la que se solicitó la información, la casa de salud no cuenta las copias del acuerdo de confidencialidad del manejo de datos de la HCE de los usuarios que han tenido acceso a la misma, debido a que los usuarios que aparecen en los registros no fueron generados en la casa de salud y tendría que remitirse a la Dirección Provincial.
4. Para solicitar procedimientos para anonimizar o seudonimizar datos de salud de la HCE y un protocolo técnico que incluya los parámetros necesarios para

garantizar la protección de datos de salud anonimizados previamente aprobados por la autoridad pertinente, comuníquese con el otro departamento que dicta estas políticas.

Como última fuente de información se analizó los datos del aplicativo web de la historia prestacional de la institución a la que el investigador tiene acceso porque es personal.

DISCUSIÓN

El Artículo 31 de la LOPDP, establece que el tratamiento de datos relacionados con la salud está regulado por legislación especializada y demás normas dictadas por la autoridad de Protección de Datos Personales en colaboración con la autoridad sanitaria nacional. Este último ha desarrollado un reglamento único para la gestión de historias clínicas, en el que se describen las funciones que deben tener para gestionarlas, incluida la interoperabilidad, es decir, mantener la comunicación entre sus sistemas informáticos y los sistemas informáticos de otras instituciones de salud. Aseguramos la confidencialidad e integridad de la información intercambiada y el acceso oportuno a la misma.

En este contexto, se puede determinar que no se cumple lo dispuesto, puesto que la institución analizada, al solicitar que se traslade la petición del investigador a la unidad médica en dónde recibió el servicio sanitario, demuestra que la información es tratada de forma independiente.

De igual manera, en el informe de la Contraloría General del Estado, expone que el proceso de auditoría DNAI-AI-0050-2017 se lo realiza en tres unidades médicas, considerando sus sistemas de manera independiente, no en conjunto como se tratan sistemas interoperables, situación que actualmente se sigue manteniendo. Esta situación incurre en incumplimiento del artículo 17 de la LOPDP, cuyas características indiquen que el titular tiene derecho a recibir sus datos personales del responsable del tratamiento o a transferirlos o transmitirlos a otro responsable, sin que el responsable pueda impedirlo, de ningún orden. Esto implica que, al ser una institución única, no puede indicar que la información se encuentra en otra unidad médica o área

administrativa con el objetivo de ralentizar el acceso, pues basta simplemente con cumplir con algunas condiciones, entre ellas el consentimiento del o de los titulares.

La información proporcionada por la institución, tales como fecha, hora y usuario que creó la HCE del investigador, no coinciden con los del aplicativo, son registros distintos con una variación significativa en el tiempo, además de intervenir usuarios automatizados, por lo tanto, no es información confiable. Uno de los principios por lo que se rige la LOPDP, es la calidad y exactitud de los datos personales; este precepto se encuentra considerado en el artículo 10, numeral h de esta Ley, en él se ha precisado que los datos personales deben caracterizarse por ser su exactitud, integridad, precisión, que se encuentren completos, sean comprobables y actualizados, tengan claridad con la finalidad de no se altere la veracidad de estos. Ante dicha situación, la calidad y exactitud esperada en el contenido con relación a lo establecido en el ordenamiento jurídico ecuatoriano no se ha producido, es decir, la manifestación de carencia del principio es clara y evidente.

En similares condiciones, la información de los usuarios que han accedido y editado la HCE no es precisa, existen diferencias significativas entre lo proporcionado y el aplicativo web; en este último se puede visualizar que existen otras instituciones diferentes a la del caso de estudio que han intervenido en el tratamiento de la información del investigador. Entre algunas de las normas de control interno que la institución ha descuidado se encuentra lo referido en la página 49 el informe de Contraloría, el cual manifiesta que no se han podido establecer procedimientos para otorgar de manera personalizada los usuarios y contraseñas a las personas internas y externas que hacen uso del sistema informático en el cual reposan las HCE, constituyéndose de esta manera en un riesgo inminente de acceso no autorizado al sistema y a sus bases de datos.

La Corte Constitucional del Ecuador, con la sentencia 1868-13-EP/20, dentro del caso N.º 1868-13-EP, “recalca que la información objeto de la acción de hábeas data es aquella relacionada con “datos personales” y/o “informes que sobre una persona” “o sus bienes” que reposen en instituciones públicas o privadas, en soporte material o electrónico”. En consecuencia, sobre la base de protección de datos personales, la

persona o el solicitante debidamente autorizado, puede exigir a dichas instituciones actualizar, corregir, eliminar o cancelar información. Todo ello se fundamenta en los derechos a la protección de datos personales, a la autodeterminación informada (Corte Constitucional del Ecuador. 2020, p. 4).

Así, en similares características, el artículo 92 de la CRE dice que toda persona tiene derecho a conocer y acceder a sus datos personales que se encuentren en las entidades públicas o privadas. Esto implica que, la institución a la que se solicitó la información debería proporcionar todos los datos solicitados por el investigador, debido a que es su competencia haberlos registrado, almacenado, y tratado de una forma eficiente de acuerdo con lo que la legislación ecuatoriana expresa. Es claro determinar que los principios de claridad y exactitud, juridicidad o seguridad no son expresamente respetados, por consiguiente, no se cumple con lo estipulado en la LOPDP.

No se proporcionan los acuerdos de confidencialidad para el manejo de datos de la HCE de los usuarios de la institución que hayan tenido acceso a esta información. En el informe de la Contraloría General del Estado DNAI-AI-0050-2017 se establece que se produce acceso sin restricciones a los datos del sistema sin acuerdos de confidencialidad firmados, y no se proporcionan instrucciones, pautas o requisitos que limiten el acceso a los datos del HCE del paciente.

El artículo 66, numeral 19, de la CRE establece el derecho a la protección de los datos personales, que comprende el acceso y decisión sobre este tipo de datos y su correspondiente protección. Cualquier recolección, almacenamiento, procesamiento, difusión o difusión de esta información requiere el permiso del titular o la autorización de la Ley.

En este contexto, se debe obtener el permiso del titular para las actividades relacionadas con el tratamiento de estos datos, de lo contrario el libre acceso y manejo de estos datos sin autorización en todas sus formas vulnera el claro derecho a la protección de datos, exceptuando por Ley u orden de un órgano judicial. Para aclarar el concepto de tratamiento de datos, por medio del Acuerdo Ministerial No. 012-2019, del Ministerio de Telecomunicaciones y de la Sociedad de la Información con Registro

Oficial 18 de 15-ago-2019 se expide la Guía para tratamiento de Datos Personales en Administración Pública; en el acápite de términos y definiciones establece que el tratamiento de datos se compone de obtener, registrar, organizar, estructurar, conservar, adaptar o modificar, extraer, consultar, utilizar, comunicar por transmisión, difundir o cualquier otra forma de acceso, cotejar o interconectar, limitar, suprimir o destruir los datos personales (Acuerdo Ministerial No. 012-2019 - Guía para tratamiento de datos personales en Administración Pública, 2019, pág. 6). Bajo este concepto, el no disponer de los acuerdos de confidencialidad por parte de la institución objeto de estudio, denota que no se cumplen ninguna de estas consideraciones que establece nuestra jurisprudencia, entendiéndose así que no se cumple otra vez más lo establecido en la LOPDP.

La investigación no pudo verificar qué medidas organizativas técnicas apropiadas implementó la institución para proteger los datos de salud en la HCE. En el informe de auditoría DNAI-AI-0050-2017, como en la información recopilada sobre la HCE del investigador, no se ha determinado que existan los procedimientos adecuados para ello, en su lugar la institución ha emitido un vago pronunciamiento poco específico sobre lo solicitado por el investigador. Por esta razón, se incurre en el incumplimiento del principio de seguridad establecido en el literal j del artículo 10 de la LOPDP.

El artículo 362 de la CRE establece que los servicios de salud son seguros y se debe garantizar la confidencialidad de la información de los pacientes. Una de las estrategias que sirve como herramienta para que pueda aplicarse el secreto de los datos es anonimizar la información. El término de anonimización, según nuestra legislación, es definido como el proceso por el cual ya no es posible establecer razonablemente una conexión entre los datos y el objeto al que se relacionan (Acuerdo Ministerial No. 012-2019, p. 5).

Por este motivo, el inciso 2 del artículo 31 de la LOPDP manifiesta que los datos relativos de la salud deberán ser anonimizados o seudonimizados para evitar que estos sean identificables. Bajo estas consideraciones, para anonimizar datos de pacientes, el siguiente párrafo del mismo artículo establece que debe existir un protocolo técnico que contenga los parámetros necesarios para asegurar la protección

de datos; su propósito es asegurar la implementación del tan esperado principio. En el informe de la auditoría DNAI-AI-0050-2017, como en la información proporcionada por la institución objeto de análisis, no se ha podido evidenciar que existe algún procedimiento técnico, administrativo o jurídico que puedan anonimizar los datos, en consecuencia, se incumple lo establecido en el ordenamiento jurídico.

CONCLUSIONES

Con la información recopilada es claro determinar que en la institución objeto de análisis, los sistemas de información no son confiables, existen brechas de seguridad en la administración de usuarios, no posee la característica de la interoperabilidad entre los sistemas que garanticen la confidencialidad y secreto profesional, no se hallan acuerdos o documentos que comprometan a los usuarios a guardar el estricto nivel de confidencialidad; en similitud de condiciones, no hay procedimientos para configurar y parametrizar los niveles de seguridad a los usuarios del sistema informático o herramientas para la anonimización o seudonimización de datos, incumpliendo lo que expone la LOPDP.

Razonablemente, hay que recalcar que, como resultado de lo expuesto en la LOPDP, es importante realizar un análisis desde la óptica de la bioética, debido a que se instaura la duda e incertidumbre hasta qué nivel se encuentran protegidos los datos personales y, si es que el consentimiento individual para dichas investigaciones podría ser autorizado por el titular; en este sentido, el legislador, para establecer su intención en una Ley, debe recurrir a expertos en el tema, como son científicos y especialistas en data Science, Big data en salud, Inteligencia Artificial, bioderecho, bioética, derecho informático, derecho en ciberseguridad y entorno digital, constitucionalistas, expertos en derechos humanos, entre otros.

Con similares consideraciones, las instituciones de salud deben esforzarse por crear políticas internas, que regulen y establezcan procedimientos y protocolos técnicos, jurídicos y administrativos que garanticen que los derechos constitucionales se cumplan, en particular, el derecho a la protección de datos personales relacionados con la salud, que se encuentra enmarcado en la LOPDP.

Es importante destacar que esta nueva Ley implementa un desarrollo normativo conjugando varias aristas del conocimiento y que ha considerado la importancia que tienen los datos personales relativos a la salud como parte del derecho de libertad que tiene cada uno de los ciudadanos.

El Estado no solo debe establecer políticas de protección de datos, sino que debe dinamizar tangiblemente el desarrollo tecnológico de la Historia Clínica Electrónica de todas las instituciones que componen el Sistema Nacional de Salud, para permitir que las personas pueden acceder a los servicios sanitarios eficientemente optimizando los recursos de cualquier naturaleza.

FINANCIAMIENTO

No monetario

AGRADECIMIENTO

A la Universidad Católica de Cuenca; por apoyar el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Abad, I., Blanco, Ó., Eduardo de Campos, F., Carnicero, J., Ceruelo, J., Chavarría, M., Elicegui, I., Fernández, A., Galán, M., Gallo, M., García, A., García, M., González Bernaldo de Quirós, F., & Ind. (2012). *Manual de salud electrónica para directivos de servicios y sistemas de salud [e-Health handbook for health services and health system managers].* Santiago de Chile: Naciones Unidas. http://hdl.handle.net/11362/3023

Acuerdo 1190. *Apruébese la utilización de los estándares Health Level Seven (HL7) y dispónerse su implementación en todas las instituciones del Sistema Nacional de Salud, observando la normativa existente del INEN [Approve the use of Health Level Seven (HL7) standards and provide for their implementation in all institutions of the National Health System, observing INEN's existing regulations*]. Registro Oficial No. 622, 19 de Enero de 2012. Recuperado de https://acortar.link/rBuYC9

Acuerdo Ministerial No. 012-2019. Guía para tratamiento de datos personales en Administración Pública [Guidelines for the treatment of personal data in Public Administration]. Recuperado de https://n9.cl/fiztr

Aguado-Renedo, C. (2010). La protección de los datos ante el Tribunal Constitucional Español [Data protection before the Spanish Constitutional Court]. *Cuestiones Constitucionales, núm. 23, julio-diciembre, 2010*, 3-25. https://bit.ly/3Qgy8WO

Alotaibi, Y. K., & Frank , F. (2017). The impact of health information technology on patient safety. *Saudi Medical Journal*, 1173-1180. https://doi.org/https://doi.org/10.15537/smj.2017.12.20631

American National Standards Institute (ANSI). (2022). HL7: Health Level Seven. https://webstore.ansi.org/sdo/hl7

Amézqueta-Goñi, C., Andérez González, A., Carnicero, J., Chavarria Díaz, M., Crespo Molina, P., Escolar Castellón, F., Falagan Mota, J. A., Garbayo Sánchez, J. A., García Rojo, M., Granado Hualde, A., Hernández Salvador, C., Iraburu Elizondo, M., Manso Montes, E., Martín Sánchez, F., Monteagudo Peña, J. L., Maldonado Segura, J. A., Nogueira Fariña, J., Reig Redondo, J., Robles Viejo, M., Sánchez García, C., Vázquez López, J. M. (2003). *De la historia clínica a la historia de salud electrónica [From the medical record to the electronic health record].* Pamplona: SEIS, Sociedad Española de Informática de la Salud. http://conganat.cim.es/seis/informes/2003/PDF/informeseis2003.pdf

Buisán i Espeleta, L. (2016). La historia clínica compartida y el ejercicio de la autonomía de las personas en sanidad [Shared medical records and the exercise of personal autonomy in health care]. *Revista de Bioética y Derecho*(37), 51-68. https://doi.org/https://doi.org/10.1344/rbd2016.37.16150

Carnicero Giménez de Azcárate, J. (2003). *Introducción. De la historia clínica a la historia de la salud electrónica. La historia clínica en la era del conocimiento* [Introduction. From the medical record to the electronic health record. The medical record in the knowledge era]. En J. Carnicero Giménez de Azcárate, *Informes SEIS De la historia clínica a la historia de salud electrónica* (pág. 401). Pamplona. http://www.seis.es

Congreso Nacional del Ecuador. (2006). *Ley Orgánica de Salud [Organic Health Law].* Quito: Segundo Suplemento del Registro Oficial 53, 29-IV-2022. https://bit.ly/3HjrWZX

Constitución de la República del Ecuador. Registro Oficial 449 de 20-oct-2008 Ultima modificación: 13-jul-2011. Recuperado de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Esquivel-Guadarrama, J. A. (2020). Pandemia 2020. Algunas consideraciones éticas [Pandemic 2020. Some ethical considerations]. *Revista Mexicana de Anestesiología, 43*(2), 168-172. https://doi.org/https://doi.org/10.35366/92878

Etreros-Huerta, J., Marco Cuenca, G., Abad Acebedo, I., & Muñoz Montalvo, J. (2009). La interoperabilidad como base de la Historia Clínica Digital del Sistema Nacional de Salud [Interoperability as the basis for the National Health System's Digital Health Record]. *Todo Hospital, 2009*(Junio), 467-474. http://eprints.rclis.org/3856/

García-Vigil, J. L. (2021). Reflections around ethics, human intelligence and artificial intelligence. *Gaceta médica de México*, 157:298-301. https://doi.org/10.24875/GMM.M21000561

Gómez-Córdoba, A., Arévalo Leal, S., Bernal Camargo, D., & Rosero de los Ríos, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia [The right to the protection of personal data, digital technologies and pandemic by COVID-19 in Colombia]. *Revista de Bioética y Derecho*, 24. https://bit.ly/3ObWyyN

IEEE Standard Glossary of Software Engineering Terminology (1990).. *IEEE Std 610.12-1990*, 1-84. https://doi.org/10.1109/IEEESTD.1990.101064

International Organization for Standardization. (2013). *International Organization for Standardization*. Retrieved from https://www.iso.org/: https://www.iso.org/standard/54534.html

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Recuperado de https://acortar.link/GdolxE

Ley Orgánica de Protección de Datos Personales. Quinto Suplemento del Registro Oficial No.459 , 26 de Mayo 2021. Recuperado de

Ley Orgánica de Salud. Registro Oficial Suplemento 423 de 22-dic.-2006 Ultima modificación: 18-dic.-2015. Recuperado de https://acortar.link/1XFLAf

Norma Técnica de Interoperabilidad Gubernamental. Acuerdo Ministerial 1062 Registro Oficial Suplemento 467 de 26-mar.-2015. Recuperado de https://acortar.link/tFWygl

Norma Técnica Historia Clínica Única Electrónica y Manual Historia Clínica Electrónica [Technical Standard Single Electronic Health Record and Electronic Health Record Manual]. Recuperado de https://acortar.link/WUJJKp

Observatorio de Bioética y Derecho. (2015). Comercializar los datos sanitarios: anonimizar no es una respuesta para la bioética [Commercializing health data: anonymizing is not an answer to bioethics]. *Revista de bioética y derecho, 33*, 1-2. https://doi.org/dx.doi.org/10.4321/S1886-58872015000100001

Reglamento para el Manejo de la Historia Clínica Electrónica. Quito: Registro Oficial Acuerdo No. 00115-2021 968, 22-III-2017. Recuperado de https://bit.ly/3NOmYXI

Reglamento para el manejo de la historia Clínica Única. Registro Oficial No. 378 , 26 de Enero 2021. Recuperado de https://acortar.link/gnFEpU

Remolina-Angarita, N. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? [Does Colombia have an adequate level of personal data protection in light of the European standard?]. *Revista Colombiana de Derecho Internacional*, 36. https://bit.ly/3zGYtHs

Siegler, E. L. (2010). The Evolving Medical Record. *Annals of Internal Medicine, 153*(10), 671. https://doi.org/10.1059/0003-4819-153-10-201011160-00012

World Health Organization. (2005). Fifty-Eighth World Health Assembly. *Resolutions and Decisions* (p. 159). Geneva: World Health Organization. https://acortar.link/OfjuIF