[Buenos Aires, martes 23 de mayo de 2023 - N° 15.527]

SALUD Y DERECHOS PERSONALÍSIMOS:

Anotaciones sobre el "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina" (ley 27.706)

SUPLEMENTO ESPECIAL

Autores:
JORGE NICOLÁS LAFFERRIERE
VERÓNICA ELVIA MELO
NOEMÍ L. NICOLAU
MATILDE PÉREZ
ROBERTO A. VÁZQUEZ FERREYRA

EL DERECHO

Contenido

PRESENTACIÓN

Salud y derechos personalísimos: Anotaciones sobre el "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina" (ley 27.706)

por Alejandro Borda(*)

El 28 de febrero de 2023, se sancionó la ley 27.706, que creó un "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina". La norma, publicada en el Boletín Oficial del 16 de marzo de 2023(1), supone un cambio significativo en lo que hace, precisamente, a los registros de historias clínicas.

Una observación preliminar, casi obvia, me lleva a señalar que la creación del llamado "Sistema Único de Registro de Historias Clínicas Electrónicas" evidencia cómo el desarrollo de las tecnologías en el ámbito médico y de salud –y en el manejo de datos– supone un desafío para los abogados. En este contexto de revolución digital e informativa, no es de extrañar que, cada vez más, debamos prestar atención a las temáticas vinculadas con el Derecho de la Salud, el derecho y la tecnología y la protección de la intimidad y de los datos personales.

No puede negarse que las tecnologías han facilitado y coadyuvado a mejorar la atención de los pacientes, durante uno de los momentos de mayor vulnerabilidad del ser humano: la enfermedad. Quizás, la coordinación de esfuerzos para el armado del registro de historias clínicas pueda ser un paso en ese camino, aunque por supuesto sería ingenuo no advertir que plantea problemáticas y dificultades.

En esa línea, una segunda observación –menos obvia quizás– se refiere a los retos que conlleva la puesta en marcha del "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina". Una respuesta preliminar aparece en la letra del legislador, que previó la implementación "en forma progresiva" (art. 2). Claro que la ley, por esencia general, deja muchas cuestiones pendientes; algunas de ellas seguramente se definan con la reglamentación, otras dependerán de las determinaciones de la autoridad de aplicación, otro tanto de los recursos y tecnologías disponibles (y de sus eventuales actualizaciones). Finalmente, muchos aspectos quedarán supeditados a la coordinación entre las diversas jurisdicciones con competencia en materia de salud, en el marco de nuestro sistema federal.

Dicho de otro modo, la creación del Programa tiene implicancias concretas en torno de las facultades y obligaciones del Estado en sus diversos niveles y respecto de los deberes de los prestatarios de salud. Será necesario trabajar con seriedad, esfuerzo, y asegurar la coordinación de recursos humanos, tecnológicos y económicos para lograr la operatividad del Programa. En ese marco, surgen muchos interrogantes: ¿Cómo se hará la implementación progresiva? ¿Se coordinará con las provincias, municipios y con la Ciudad Autónoma de Buenos Aires? ¿Podría afectarse el reparto de competencias en el esquema constitucional federal en materia de salud entre el Estado nacional, las provincias y la Ciudad Autónoma de Buenos Aires? ¿Se coordinará con los hospitales, consultorios u otros servicios privados? ¿Cómo se realizarán las capacitaciones al personal sanitario? ¿Qué responsabilidades pueden acarrear las disposiciones de la norma para los establecimientos que prestan servicios salud? Desde luego, además, se requerirá el diseño de programas para la capacitación del personal, en todos los niveles de gobierno, tanto en el sector de salud público como en el ámbito privado... Aquí también aparece una inquietud adicional, ¿es posible lograr una capacitación medianamente homogénea?

Tercero, desde luego, la ley 27.706 tendrá efectos concretos en términos de los derechos de los pacientes. En especial, si se tiene presente que la información consignada en una historia clínica es sensible e íntima. Aquí, aparece un aluvión de preguntas: ¿Cómo pueden resguardarse los datos personales contenidos en las historias clínicas y en el Sistema Único de Registro de Historias Clínicas Electrónicas? ¿Los pacientes deberían prestar su consentimiento para que sus datos queden insertados en el registro? ¿Qué mecanismos se emplearán para el resguardo de la intimidad del paciente? ¿Cómo podrá el paciente, titular de los datos consignados, acceder a la información registrada? ¿Podrán estas historias hacerse valer fuera del país? ¿Cómo se protegerá la inalterabilidad de la información? ¿Cómo interactúa la nueva norma con la ley 25.326, de protección de los datos personales? ¿Qué sistemas de *software* se utilizarán para su implementación? ¿Podrían estos sistemas ser hackeados? ¿Se buscará contar con *backup* para el caso de la pérdida o extravío de la información digital? ¿Qué mecanismos de seguridad se utilizarán para prevenir el robo o la filtración de la información sensible?

No albergo ninguna duda de que este aspecto, por la relevancia de los derechos personalísimos involucrados, es el más importante de todos. Adviértase que resulta necesario resguardar tal información no solo de filtraciones generadas por quienes han accedido a esos datos personales de manera lícita, sino también de la deleznable acción de los delincuentes informáticos que lucran con ella.

Con tantos interrogantes, y mientras aguardamos la reglamentación de la norma –según la ley, se ha fijado un plazo de 90 días desde su publicación en el Boletín Oficial para que el Poder Ejecutivo dicte el decreto correspondiente– parece inevitable abordar y conocer el texto de la ley 27.706.

Con eso en mente, desde la editorial El Derecho, nos propusimos trabajar en un número especial destinado a reflexionar. Contamos para eso con especialistas en la temática, los doctores, Jorge Nicolás Lafferriere, Verónica Elvia Melo, Noemí L. Nicolau, Matilde Pérez y Roberto A. Vázquez Ferreyra. Cada uno de ellos, nos adentra en las aristas, aciertos, dificultades y dudas del "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina" y nos abren los ojos ante nuevos interrogantes.

Sin más que decir, con orgullo, comparto con ustedes este nuevo suplemento.

VOCES: HISTORIA CLÍNICA - PROTECCIÓN DE DATOS PERSONALES - TECNOLOGÍA - PERSONA - CONSTITUCIÓN NACIONAL - INTIMIDAD - DERECHOS Y GARANTÍAS CONSTITUCIONALES - INFORMÁTICA - INTELIGENCIA ARTIFICIAL - DERECHOS PERSONALÍSIMOS - ORDEN PÚBLICO - HÁBEAS DATA - DERECHOS HUMANOS - SECRETO PROFESIONAL - DAÑOS Y PERJUICIOS - DAÑO MORAL - DAÑO PSÍQUICO - RESPONSABILIDAD CIVIL - MÉDICO - MEDICAMENTOS - CONTRATOS - OBLIGACIONES - CÓDIGO CIVIL Y COMERCIAL - ACTOS Y HECHOS JURÍDICOS - COMERCIO E INDUSTRIA - POLÍTICAS PÚBLICAS - SALUD PÚBLICA - CONSENTIMIENTO - PRUEBA - CARGA DE LA PRUEBA - HOSPITALES Y SANATORIOS - OBRAS SOCIALES - DERECHOS DEL CONSUMIDOR - MEDICINA PREPAGA - PROFESIONALES DE LA SALUD

(*) Director de la editorial El Derecho.

(1) La ley 27.706 fue promulgada por el decreto 144/2023 (BO 16/3/2023).

Argentina sanciona la ley 27.706 para crear un sistema único de registro de historias clínicas electrónicas

por Jorge Nicolás Lafferriere(*)

Sumario: El contenido de la ley. – Primeras consideraciones sobre la ley. *a) ¿Se justifica la creación compulsiva de una base con los datos de salud de toda la población? b) La cuestión de la seguridad de los datos. c) La implementación de la ley y su impacto en la tarea de los profesionales de la salud. d) Otras cuestiones.*

El 16 de marzo de 2023 se publicó en el Boletín Oficial de la República Argentina la ley 27706 que crea el Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina, que había sido sancionada el 28 de febrero de 2023.

El contenido de la ley

La ley consta de 11 artículos organizados en 3 capítulos. El primer capítulo se refiere a la finalidad del programa: "Instaurar, en forma progresiva, el Sistema Único de Registro de Historias Clínicas Electrónicas, respetando lo establecido por el Capítulo IV de la ley 26.529 de Derechos del Paciente en su relación con los Profesionales e Instituciones de la Salud y por la ley 25.326 de Protección de los Datos Personales y sus modificatorias" (art. 1).

El artículo 2 enumera las atribuciones de la autoridad de aplicación de la ley, que será determinada por el Poder Ejecutivo. Entre esas atribuciones se encuentran definiciones de decisiva importancia para conocer cómo funcionará el programa en lo concreto. En efecto, la autoridad de aplicación debe: "a) Crear y conformar con las provincias y la Ciudad Autónoma de Buenos Aires la estructura organizativa del Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina y reglamentar su implementación y su progresivo funcionamiento; b) Determinar las características técnicas y operativas de la informatización y digitalización de las historias clínicas del sistema de salud de la República Argentina; c) Elaborar un protocolo de carga de historias clínicas, así como diseñar e implementar un software de historia clínica coordinando la implementación interjurisdiccional, ajustándose a lo dispuesto por la presente y por las leyes 26.529 y 25.326 y sus normas modificatorias y reglamentarias; d) Generar un marco de interoperabilidad entre los sistemas que se encuentren en funcionamiento con los sistemas a crear, tanto en el sector público, privado y del ámbito de la seguridad social; e) Instalar el software de forma gratuita en todos los hospitales públicos, nacionales, provinciales y municipales; y, en la forma que se establezca por vía reglamentaria, en los centros de salud privados y de la seguridad social…". Además, la autoridad de aplicación debe proveer asistencia técnica y financiera a las provincias, coordinar recursos, crear una comisión interdisciplinaria de expertos y capacitar al personal sanitario.

El capítulo II regula lo que denomina el Sistema Único de Registro de Historias Clínicas Electrónicas. Según el artículo 3, "en el Sistema Único de Registro de Historias Clínicas Electrónicas se deja constancia de toda intervención médico-sanitaria a cargo de profesionales y auxiliares de la salud, que se brinde en el territorio nacional, ya sea en establecimientos públicos del sistema de salud de jurisdicción nacional, provincial o municipal, y de la Ciudad Autónoma de Buenos Aires, como en establecimientos privados y de la seguridad social". En el artículo 4 se afirma que el Sistema Único "debe contener los datos clínicos de la persona o paciente, de forma clara y de fácil entendimiento, desde el nacimiento hasta su fallecimiento". Luego se formulan aclaraciones en el sentido de que los datos no pueden ser alterados (art. 4) y de que el sistema garantiza el acceso a la base de datos desde cualquier lugar del territorio nacional (art. 5). Se explican las características del Sistema Único (art. 6) y se formulan algunas definiciones. En general, se enfatiza la importancia de la privacidad y confidencialidad de los datos.

El capítulo III se titula "Historia clínica electrónica" y señala en su artículo 8: "El paciente es titular de los datos y tiene en todo momento derecho a conocer la información en la Historia Clínica Electrónica que es el documento digital, obligatorio, con marca temporal, individualizada y completa, en el que constan todas las actuaciones de asistencia a la salud efectuadas por profesionales y auxiliares de la salud a cada paciente, refrendadas con la firma digital del responsable […]. Forman parte los consentimientos informados, las hojas de indicaciones médicas y/o profesionales, las planillas de enfermería, los protocolos quirúrgicos, las prescripciones dietarias, certificados de vacunación, los estudios y prácticas realizadas, rechazadas o abandonadas…". El artículo 9 se refiere a los fondos para financiar el cumplimiento del programa y el artículo 10 señala el deber del Poder Ejecutivo de reglamentar la ley en 90 días. El artículo 11 es de forma.

Primeras consideraciones sobre la ley

Más allá de las buenas intenciones que subyacen a la ley y que se vinculan con los beneficios de contar con una historia clínica disponible en cualquier lugar del país para el paciente y el profesional de la salud, subsisten importantes dudas e interrogantes sobre la ley.

a) ¿Se justifica la creación compulsiva de una base con los datos de salud de toda la población?

La ley 27.706 reafirma que la historia clínica electrónica es propiedad del paciente (art. 8), tal como ya lo disponía la ley 26.529. Ahora bien, más allá de esa afirmación, esta ley habilita al Estado a formar una gran base de datos con las historias clínicas de toda la población a través del llamado Sistema Único de Registro de Historias Clínicas. Ello genera una razonable preocupación por los usos que pueda tener esa base.

Al respecto, cabe preguntarse si formar tal base con los datos de todos los pacientes de manera compulsiva es proporcionado a los fines en juego o si se debía considerar la posibilidad de que sean los pacientes quienes decidan ingresar sus historias clínicas. La ley 27.706 pre-

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *La indemnización correspondiente por la no obtención del consentimiento informado en la praxis médica*, por Roberto A. Vázquez Ferreyra, ED, 197-709; *Historia clínica. Encuadre probatorio. Responsabilidad médica. Responsabilidad omisiva*, por Lucía Graciela Savarese, ED, 216-642; *El derecho a la salud como derecho social. Garantía de la dignidad del hombre*, por Violeta Castelli, EDA, 2007-743; *El plazo de la prescripción liberatoria en materia de responsabilidad médica en los hospitales de la Ciudad Autónoma de Buenos Aires*, por Inés Amura, Esteban Centanaro y Juan Pablo Rodríguez, ED, 234-708; *Responsabilidad médica por mala praxis*, por Mariano Gagliardo, ED, 251-465; *Los médicos y el consentimiento informado (Necesarias precisiones sobre el tema en el marco del nuevo CCC)*, por Marcelo J. López Mesa, ED, 266-703; *La doctrina de la "real malicia" y el derecho a la información sobre cuestiones médicas*, por María Angélica Gelli, ED, 277; *Consentimiento informado de las personas con discapacidad en tratamientos médicos*, por Nicolás Pildayn y Marina M. Sorgi Rosenthal, ED, 279; *La protección de los datos personales en internet (una tarea ineludible)*, por Esteban Ruiz Martínez, ED, 284-726; *Datos personales: Google se asocia con el sistema de salud más importante de Estados Unidos*, por Laura Belén Yachelini, ED, 286-618; *El médico y la virtud de la prudencia en tiempos de pandemia*, por Germán Calabrese, ED, 289-1581; *Odontólogos. Responsabilidad civil profesional en tiempos de pandemia*, por Dante Gómez Haiss, 289-1434; *La responsabilidad del médico especialista*, por Milton H. Kees, ED, 290; *La regulación del derecho a la imagen y el régimen de protección de datos de carácter personal. Ciertas "fricciones" entre ambos regímenes*, por Guillermo F. Peyrano, ED, 290-637; *Responsabilidad del médico: necesidad de deslindar el casus de la no culpa*, por Federico Ossola y Julieta Bollero Hauser, ED, 291; *El derecho a la información de salud y el hábeas data específico*, por Eduardo Molina Quiroga, ED, 294; *Derecho a la intimidad de los datos de salud*, por Julián Prieto, ED, 300. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Director del Centro de Bioética, Persona y Familia. Abogado (UBA), Doctor en Ciencias Jurídicas (UCA). Profesor Titular Ordinario de Principios de Derecho Privado e Instituciones de Derecho Civil (UCA). Profesor Adjunto Regular de Derecho Civil (UBA). Este trabajo fue publicado en la página web del Centro de Bioética, Persona y Familia, el 19 de marzo de 2023, disponible en https://centrodebioetica.org/argentina-sanciona-la-ley-27-706-para-crear-un-sistema-unico-de-registro-de-historias-clinicas-electronicas/#:~:text=El%2016%20de%20marzo%20de,28%20de%20febrero%20de%202023 (fecha de consulta: 27/4/2023).

supone que todos los pacientes están de acuerdo con ser incluidos en el Registro Único. Incluso la ley no ha previsto nada sobre la posibilidad de un paciente de decidir no participar del Registro Único. La ley se podría haber diseñado sobre la base de una participación voluntaria de los pacientes.

Lo mismo puede decirse sobre el Registro Único y el respeto a las distintas instituciones implicadas y la posibilidad de participar voluntariamente del registro.

Igualmente, si se consideraba necesario formar ese Registro Único, cabe también precisar mucho mejor qué datos deben compartirse y qué datos no.

Si el objetivo es la portabilidad de la historia clínica, de modo que el paciente pueda llevarla a los distintos lugares donde se va a atender, es clave el trabajo de interoperabilidad entre sistemas. A su vez, la privacidad y seguridad del paciente debería ser el punto de partida de toda la iniciativa aplicando el principio de subsidiariedad. Así, antes que decidir unificar "todos" los registros de las historias clínicas del país, se deberían especificar mejor las reglas que rigen la privacidad y seguridad de los datos de los pacientes.

Para contar con otras referencias, en Estados Unidos se aprobó la ley sobre tecnología referida a la información en salud para la salud económica y clínica (Health Information Technology for Economic and Clinical Health Act –HITECH–) del año 2009 con la finalidad de promover la adopción y el uso significativo de tecnologías de información en salud. Esta ley dispuso incentivos financieros para adoptar la historia clínica electrónica y aumentó las penas por violaciones a la seguridad y privacidad de los datos. El presupuesto para implementar la HITECH fue de 25.000 millones de dólares y con esos fondos se financió el programa Uso Significativo (Meaningful Use Program), que otorgó incentivos económicos para adoptar los sistemas electrónicos. En 2018, este programa cambió su denominación por el de Promoción de la Operabilidad (Promoting Operability Program)[1].

b) La cuestión de la seguridad de los datos

La ley 27.705 en distintos pasajes reafirma la importancia de respetar la confidencialidad de la información y la ley 25.326. Además de la mención a esa ley en el artículo 1, el tema aparece en otros artículos, como el artículo 2.c cuando se refiere al "protocolo de carga de historias clínicas" y al "software de historia clínica". Al referirse al Sistema Único de Registro, el artículo 6 reitera: "b) La información clínica contenida en el Sistema Único de Registro de Historias Clínicas Electrónicas, su registro, actualización o modificación y consulta se efectúan en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad, acceso y trazabilidad". Entre las definiciones del artículo 7, incluye: "d) Seguridad: preservación de la confidencialidad, integridad y disponibilidad de la información, además de otras propiedades, como autenticidad, responsabilidad, no repudio y fiabilidad; e) Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información y/o sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad, dejando rastro del respectivo acceso". Y el artículo 4 sostiene: "… La información suministrada no puede ser alterada, sin que quede registrada la modificación pertinente, aun en el caso de que tuviera por objeto subsanar un error acorde a lo establecido en la ley 25.326 de Protección de Datos Personales y sus modificatorias". En el artículo 8 reitera: "El almacenamiento, actualización y uso se efectúa en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad y acceso, de conformidad con la normativa aprobada por la autoridad de aplicación de la presente ley, como órgano rector competente".

Sin embargo, las dudas se presentan en relación con la efectiva seguridad de los sistemas, más allá de los términos de la ley. Tengamos en cuenta que los datos personales de salud configuran datos sensibles y que la actual ley de protección de datos personales (Ley 25.326 del año 2000) no ha sido actualizada.

Además, las penas por incumplimiento de las disposiciones sobre protección de datos personales son bajas y casi inexistentes en la práctica. Un tipo de norma que se propone armar una base unificada con los datos de salud de todos los argentinos debería ir precedida por normas mucho más precisas sobre derechos del paciente a la privacidad y confidencialidad de la información de salud.

Para tomar en cuenta experiencias comparadas, también en los Estados Unidos en 1996 se aprobó la ley sobre Portabilidad y Responsabilidad de los Datos del Seguro de Salud (Health Insurance Portability and Accountability Act –HIPAA–), que dio lugar a una regla sobre privacidad y una regla sobre seguridad que son muy estrictas y que van acompañadas por un sistema de supervisión de cumplimiento (*compliance*), deberes de informar las violaciones a la seguridad e importantes sanciones. La regla de privacidad fija los estándares para que los pacientes comprendan y controlen cómo se utiliza su información de salud y procura un balance entre la protección de la privacidad y el necesario flujo de información para que se brinde una buena atención. Por su parte, la regla sobre seguridad apunta a asegurar la confidencialidad, integridad y disponibilidad de la información, detectar y tomar medidas por anticipado contra las amenazas a la seguridad de la información, proteger contra usos no autorizados y certificar el cumplimiento de las reglas. Las sanciones económicas por violar la HIPAA se ubican entre 50.000 y 250.000 dólares, y también existen sanciones penales para los casos más graves. Por su parte, también la ley HITECH estableció un sistema de sanciones, con una pena máxima de 1,5 millones de dólares por violaciones a sus disposiciones. La HITECH puso también normas más rigurosas para el uso de información de salud en marketing y búsquedas de fondos, expandió los derechos del paciente para impedir que se compartan sus datos y fijó los usos que requerían autorización. También estableció la responsabilidad directa de las empresas por violación a la ley de privacidad.

c) La implementación de la ley y su impacto en la tarea de los profesionales de la salud

La ley no es inmediatamente operativa, pues requiere de acuerdos previos con las provincias y la Ciudad Autónoma de Buenos Aires, y del desarrollo de los sistemas informáticos que permitan la efectiva implementación de la historia clínica electrónica.

Al respecto, en la experiencia internacional se verifican intentos de generar interoperabilidad entre los sistemas informáticos de los servicios de salud a fin de facilitar el acceso en distintos lugares a los registros médicos, y ello no ha sido tan fácil. En el caso de los Estados Unidos, antes que a través de una norma vinculante, ello se hizo a través de programas de incentivos para que las instituciones adopten protocolos de interoperabilidad (HITECH).

Además, hay problemas vinculados con la mayor carga de trabajo que significa completar estas historias clínicas electrónicas, a lo que se añaden dificultades asociadas con los errores y daños por deficiente gestión de la interoperabilidad. Se puede ver al respecto el libro de Robert Watcher sobre el "doctor digital" ("The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine's Computer Age", McGraw Hill, 2015).

Según un trabajo publicado en 2019, las barreras más mencionadas en la literatura científica sobre la implementación de sistemas de historia clínica electrónica eran: limitado conocimiento sobre telesalud, falta de equipamiento, problemas de financiamiento de la soluciones de telesalud, conocimiento, seguridad, motivación, accesibilidad, servicios inadecuados a las necesidades de los usuarios, confidencialidad, problemas en la inserción de los sistemas en las estructuras organizacionales y aumento de la carga de trabajo[2]. El mismo estudio señala algunos facilitadores de la adopción de la historia clínica electrónica: que sea sencillo de usar, que mejore la comunicación, motivación, que esté integrado a la atención de

(1) Véase The HIPAA Journal, "What is the HITECH Act?", disponible en https://www.hipaajournal.com/what-is-the-hitech-act/#:~:text=The%20HITECH%20Act%20encouraged%20healthcare,HIPAA%20Privacy%20and%20Security%20Rules (fecha de consulta: 27/4/2023).

(2) Schreiweis B., Pobiruchin M., Strotbaum V., Suleder J., Wiesner M., Bergh B., "Barriers and Facilitators to the Implementation of eHealth Services: Systematic Literature Analysis", *J Med Internet Res.*, 2019, Nov. 22;21(11): e14197. DOI: 10.2196/14197. PMID: 31755869; PMCID: PMC6898891.

salud, que se involucren los actores relevantes, que haya recursos y que sea amigable para el usuario.

d) Otras cuestiones

La redacción de la norma no ha tratado de forma adecuada lo referido a las situaciones de restricción a la capacidad. Al respecto, dispone el artículo 8: "... En caso de incapacidad del paciente o imposibilidad de comprender la información a causa de su estado físico o psíquico, la misma debe ser brindada a su representante legal o derecho habientes, conforme lo establecido por la ley 25.326 de protección de los datos personales y sus modificatorias…". Ante todo, la ley 27.706 utiliza una redacción imprecisa cuando señala el supuesto de "imposibilidad de comprender la información", que tendrá impacto en el momento en que un profesional de salud tenga que determinar si la persona puede o no comprender la información. Igualmente, no regula el caso de restricciones a la capacidad, que es el supuesto genérico previsto en el Código Civil y Comercial. Los casos de incapacidad son muy excepcionales (art. 32, CCC).

VOCES: HISTORIA CLÍNICA - PROTECCIÓN DE DATOS PERSONALES - TECNOLOGÍA - PERSONA - CONSTITUCIÓN NACIONAL - INTIMIDAD - DERECHOS Y GARANTÍAS CONSTITUCIONALES - INFORMÁTICA - INTELIGENCIA ARTIFICIAL - DERECHOS PERSONALÍSIMOS - ORDEN PÚBLICO - HÁBEAS DATA - DERECHOS HUMANOS - SECRETO PROFESIONAL - DAÑOS Y PERJUICIOS - DAÑO MORAL - DAÑO PSÍQUICO - RESPONSABILIDAD CIVIL - MÉDICO - MEDICAMENTOS - CONTRATOS - OBLIGACIONES - CÓDIGO CIVIL Y COMERCIAL - ACTOS Y HECHOS JURÍDICOS - COMERCIO E INDUSTRIA - POLÍTICAS PÚBLICAS - SALUD PÚBLICA - CONSENTIMIENTO - PRUEBA - CARGA DE LA PRUEBA - HOSPITALES Y SANATORIOS –OBRAS SOCIALES - DERECHOS DEL CONSUMIDOR - MEDICINA PREPAGA - PROFESIONALES DE LA SALUD

Historia clínica electrónica. Reflexiones preliminares acerca de la ley 27.706

por Noemí L. Nicolau(*)

Sumario: 1. Aspectos generales. – 2. Historia clínica electrónica. – 3. El Programa Federal. – 4. La seguridad del sistema y el derecho a la intimidad del paciente. – 5. Los profesionales obligados. – 6. La experiencia en otros países. – 7. Conclusión.

1. Aspectos generales

La publicación de la ley 27.706, que estructura el "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina", es una oportunidad para reflexionar, en el marco del Derecho de la salud, sobre la historia clínica, documento esencial en la relación entre paciente y equipo de salud, y sobre la necesidad de concretar su informatización.

En el derecho nacional, la historia clínica está definida y regulada en los artículos 12 y siguientes de la ley 26.529 de derecho de los pacientes, que han sido reglamentados según decreto 1089/2012. La nueva ley ratifica la vigencia de esas normas y estructura el régimen de un registro nacional de historias clínicas electrónicas que se organizará en un proceso consensuado con las provincias y la Ciudad Autónoma de Buenos Aires, como corresponde.

La ley que comentamos fue aprobada en Senadores el día 5 de noviembre de 2020. La Comisión de Salud y Sistemas, Medios de Comunicación, Libertad de Expresión y de Presupuesto y Hacienda informó que tenía los Proyectos de los senadores Roberto Basualdo, Silvina García Larraburu, Silvia Elías de Pérez, y otros, Antonio Rodas y Maurice Closs. El proyecto del último senador enunciado es el que se adoptó. En sus fundamentos se describe el largo camino que el tema debió recorrer en el Senado de la Nación. En 2017, hubo dictamen de Comisión que perdió estado parlamentario, el que, a su vez, reproducía una versión de 2015 de la misma Comisión. En noviembre de 2020, finalmente, el proyecto en Senadores fue aprobado y pasó a la Cámara de Diputados que lo aprobó después de más de dos años. La ley fue publicada en el Boletín Oficial el 16 de marzo del corriente año 2023. Largos tiempos para cuestiones que deberían interesar a la población del país, sin distinciones. Al momento de escribir este trabajo está corriendo el plazo para el dictado de la norma reglamentaria que, en este caso, parece imprescindible.

La nueva normativa consta de tres capítulos. En el Capítulo I, traza los lineamientos del "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina" y pone la implementación de dicho Programa a cargo de un funcionario nacional que deberá ser designado al efecto. En el Capítulo II, organiza el "Sistema Único de Registro de Historias Clínicas Electrónicas" y establece las pautas concretas que tienden a lograr su seguridad. En el Capítulo III, define la historia clínica (HC) electrónica y regula algunos aspectos particulares.

Sin duda, es una iniciativa bienvenida en el camino de la modernización e informatización del país y de la salud pública, aun cuando se sabe que el camino será muy largo y despierta inquietudes, en algunos aspectos, que se analizarán a continuación.

2. Historia clínica electrónica

La HC que ahora la nueva ley ordena informatizar está regulada en el referido artículo 12 y siguientes de ley de derechos del paciente(1). De manera sintética y precisa

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *La indemnización correspondiente por la no obtención del consentimiento informado en la praxis médica*, por Roberto A. Vázquez Ferreyra, ED, 197-709; *Historia clínica. Encuadre probatorio. Responsabilidad médica. Responsabilidad omisiva*, por Lucía Graciela Savarese, ED, 216-642; *El derecho a la salud como derecho social. Garantía de la dignidad del hombre*, por Violeta Castelli, EDA, 2007-743; *El plazo de la prescripción liberatoria en materia de responsabilidad médica en los hospitales de la Ciudad Autónoma de Buenos Aires*, por Inés Amura, Esteban Centanaro y Juan Pablo Rodríguez, ED, 234-708; *Responsabilidad médica por mala praxis*, por Mariano Gagliardo, ED, 251-465; *Los médicos y el consentimiento informado (Necesarias precisiones sobre el tema en el marco del nuevo CCC)*, por Marcelo J. López Mesa, ED, 266-703; *La doctrina de la "real malicia" y el derecho a la información sobre cuestiones médicas*, por María Angélica Gelli, ED, 277-47; *Consentimiento informado de las personas con discapacidad en tratamientos médicos*, por Nicolás Pildayn y Marina M. Sorgi Rosenthal, ED, 279-726; *La protección de los datos personales en internet (una tarea ineludible)*, por Esteban Ruiz Martínez, ED, 284-726; *Datos personales: Google se asocia con el sistema de salud más importante de Estados Unidos*, por Laura Belén Yachelini, ED, 286-618; *El médico y la virtud de la prudencia en tiempos de pandemia*, por Germán Calabrese, ED, 289-1581; *Odontólogos. Responsabilidad civil profesional en tiempos de pandemia*, por Dante Gómez Haiss, 289-1434; *La responsabilidad del médico especialista*, por Milton H. Kees, ED, 290-809; *La regulación del derecho a la imagen y el régimen de protección de datos de carácter personal. Ciertas "fricciones" entre ambos regímenes*, por Guillermo F. Peyrano, ED, 290-637; *Responsabilidad del médico: necesidad de deslindar el casus de la no culpa*, por Federico Ossola y Julieta Bollero Hauser, ED, 291-514; *El derecho a la información de salud y el hábeas data específico*, por Eduardo Molina Quiroga, ED, 294-972; *Derecho a la intimidad de los datos de salud*, por Julián Prieto, ED, 300. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Doctora en Derecho y Ciencias Sociales. Profesora Honoraria de la Universidad Nacional de Rosario. Directora del Centro de Investigaciones en Derecho civil de la Facultad de Derecho Universidad Nacional de Rosario. Exdirectora de la Maestría en Derecho Civil de la misma Facultad.

(1) Acerca de los aspectos jurídicos de la HC puede verse: Domínguez Luelmo, A., *Derecho Sanitario y responsabilidad médica*, Lex Nova, Valladolid, 2003, p. 397 y ss.; Wierzba, S., "La historia clínica en la ley 26.529", en Carlos A. G. (dir.), *Daño a la persona y al patrimonio*, Nova tesis, Rosario, 2011, p. 303; Souto Paz, J. A., *Perspectiva jurídica de la historia clínica, Informaciones psiquiátricas:*

está definida como el "documento obligatorio cronológico, foliado y completo en el que conste toda actuación realizada al paciente por profesionales y auxiliares de la salud". En el artículo 13, se admite la informatización "siempre que se arbitren todos los medios que aseguren la preservación de su integridad, autenticidad, inalterabilidad, perdurabilidad y recuperabilidad de los datos contenidos en la misma, en tiempo y forma". Esta definición se complementa ahora con el artículo 8º de la ley 27.706 a fin de adaptarla a la Historia Clínica Electrónica (HCE) diciendo que es "el documento digital, obligatorio, con marca temporal, individualizada y completa, en el que constan todas las actuaciones de asistencia a la salud efectuadas por profesionales y auxiliares de la salud a cada paciente, refrendadas con la firma digital del responsable".

De modo que, según las definiciones de ambas leyes y la mayoría de la doctrina nacional, la HC es un documento, aun cuando en alguna oportunidad se la definió como un conjunto de documentos[2]. Debemos entender que es un documento que puede y debe tener como anexos otros diferentes documentos (consentimiento, exámenes de laboratorio, etc.). En la medida en que sea obligatoria la firma del profesional actuante, tal como lo exige el artículo 8 para la HCE, recién citado, será un instrumento privado de acuerdo con el artículo 287 del Código Civil y Comercial de la Nación con los alcances del artículo 288, según el cual la firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde.

Las definiciones apuntadas caracterizan a ese documento, en primer lugar, como *obligatorio* lo cual supone que, en la relación del paciente con los equipos de salud, estos asumen una determinada obligación legal, confeccionar la HC y registrar en ella todo acto médico, obligación que deben cumplir a fin de no incurrir en responsabilidad civil por incumplimiento obligacional, sin perjuicio de otras sanciones, como se verá.

La ley 26.529 establece tres requisitos que debe reunir ese documento obligatorio: ser *cronológico*, es decir, no se puede antedatar ni posdatar, *foliado, y completo*. Para ser completo debe reunir los requisitos objetivos establecidos en el artículo 15 de la ley y su reglamentación (tales como nombre y apellido del paciente, documento nacional de identidad, sexo, edad, dirección y aquellos antecedentes sociales, y/u otros que se consideren importantes para su tratamiento, fecha y hora de la actuación).

La nueva norma exige para la HCE que tenga firma digital del responsable[3] y además que posea *marca temporal, individualizada y completa*. La marca de tiempo es la asignación de la fecha y la hora por medios electrónicos a un documento electrónico.

En especial interesa que en toda HC conste: "Todo acto médico realizado o indicado, sea que se trate de prescripción y suministro de medicamentos, realización de tratamientos, prácticas, estudios principales y complementarios afines con el diagnóstico presuntivo y en su caso de certeza, constancias de intervención de especialistas, diagnóstico, pronóstico, procedimiento, evolución y toda otra actividad inherente, en especial ingresos y altas médicas", según exige el artículo, 15 inciso f), de la ley 26.529.

En ese sentido, la HC en su faz más importante es un documento en el que se materializa la labor intelectual del profesional de la medicina, puesto que debe describir con precisión la anamnesis que efectúa al paciente, lo cual depende de su formación y su saber. Ese es el punto en el que debe juzgarse la completitud de la HC, su claridad y la mayor y mejor información brindada por el médico[4].

Aceptado que la HC es un documento, a los efectos probatorios hay que distinguir si se trata de un instrumento particular no firmado, de un instrumento privado o de un instrumento público. Si la HCE no tiene firma digital, es un instrumento particular no firmado; si la tiene, cumpliendo la exigencia legal, es un instrumento privado, y si reúne el requisito previsto en el artículo 6, inciso g), de la nueva ley, es un instrumento público porque cumple con los recaudos del artículo 290 del Código Civil y Comercial de la Nación y porque así lo consigna también el inciso g) de la norma comentada: "La información contenida en el Sistema Único de Registro de Historias Clínicas Electrónicas constituye documentación auténtica y, como tal, es válida y admisible como medio probatorio, haciendo plena fe a todos los efectos, siempre que se encuentre autenticada"[5].

3. El Programa Federal

En el Capítulo I, la implementación del Programa se pone a cargo de un funcionario nacional que deberá ser designado al efecto. Se le atribuyen facultades y se determinan los parámetros que deberá cumplir al diseñar el sistema único de registro.

El legislador ha fijado un amplio ámbito de aplicación de la norma, pues, determina que es aplicable a toda intervención médico-sanitaria, ya sea a cargo de profesionales como de auxiliares de la salud. Se aplicará en todo el territorio nacional, ya sea en establecimientos públicos del sistema de salud de jurisdicción nacional, provincial o municipal, y de la Ciudad Autónoma de Buenos Aires. Se aplicará también a establecimientos privados y de la seguridad social. La autoridad nacional deberá coordinar con las autoridades provinciales para lograr la aplicación efectiva y puesta en marcha del programa.

Esa autoridad nacional debe elaborar un *protocolo de carga de historias clínicas* y diseñar e implementar un *software de historia clínica* coordinando la implementación interjurisdiccional. El legislador ha sido exigente en relación a ese trabajo de informatización. Dispone que la autoridad nacional, en la implementación del sistema, controle el cumplimiento de lo dispuesto por las leyes 26.529 de derechos del paciente y 25.326 de protección de datos personales, sus normas modificatorias y reglamentarias. Esta es una cuestión central del sistema y una preocupación que se advierte en la legislación comparada porque impacta en forma directa en los derechos personalísimos del paciente y, en particular, en el derecho a la privacidad.

Asimismo, se le otorgan facultades para crear una Comisión Interdisciplinaria de expertos a fin de coordinar la implementación de la ley entre los sistemas involucrados. Es de esperar que la comisión se constituya de manera interdisciplinaria, en la realidad, con la integración de, al menos, un número equilibrado de médicos, bioeticistas, abogados, expertos informáticos.

Respecto de los aspectos tecnológicos e informáticos, dado el carácter de este trabajo, solo nos interesa señalar, reiteradamente, el necesario y extremo cuidado que deberán tener quienes implementen el sistema a fin de lograr que en su uso se respeten los derechos de los pacientes, en general, y en el tratamiento de datos personales, que en su mayoría serán datos sensibles[6].

Por tanto, es importante regular en forma cuidadosa las operaciones que se pueden llevar a cabo en el Registro, que son: registro, actualización, modificación y consulta, porque cada una de estas operaciones conlleva el riesgo de afectar el sistema e, incluso, de permitir la manipulación de los datos, por lo que el acceso al Registro debe ser protegido al máximo. Por tal razón, el artículo 5 garantiza

---

Publicación científica de los Centros de la Congregación de Hermanas Hospitalarias del Sagrado Corazón de Jesús, ISSN 0210-7279, N° 191, 2008, p. 73; da Costa Carballo, C. M., "Otros documentos: la historia clínica", *Documentación de las ciencias de la información*, 20, 41/63, Servicio de publicaciones, Universidad complutense de Madrid, Madrid, 1997; Broggi, M. A., "La historia clínica", Barcelona, *Annales de Medicina* 1999; 82: 338-340; Pagliuca, F. E., "Mala praxis: La prueba de la culpa a través de la historia clínica", *SJA* 20/11/2019, 49; Papillú, J., "La valoración de la prueba en la responsabilidad civil de los médicos (omisiones en la historia clínica)", *RCCyC 2023* (abril), 222.

(2) Se refieren a "conjunto de documentos" los Proyectos presentados a la Cámara de Diputados por el diputado Roberto Basualdo y por la diputada Silvia Elías de Pérez y otros.

(3) En nuestro país está regulada por la ley 25506, que la define en su artículo 2°: "Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma".

(4) Molina Quiroga, E., "El derecho a la información de salud y el habeas data específico en la legislación argentina", SJA 29/11/2017, 39, TR LALEY AR/DOC/4247/2017.

(5) La calificación adecuada de un documento tiene importancia en la práctica, porque la determinación de la autoría y, por tanto, de la obligatoriedad, es diferente, si se trata de un instrumento privado o un instrumento público.

(6) Precisamente los datos sensibles, aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual, deben ser protegidos porque pertenecen a la esfera más privada de la vida de la persona e indudablemente muchos de ellos se registran por necesidad en las historias clínicas.

a los pacientes que "la consulta de sus datos quedará restringida a quien esté autorizado".

Además, el artículo 6 de la ley exige que para el acceso a una HC se garanticen los mecanismos informáticos de autenticación de las personas, agentes, profesionales y auxiliares de la salud que intervengan en el Sistema Único de Registro. La autenticación es un mecanismo de seguridad que permite el acceso a la información en tres niveles diferentes: el de consulta, el de consulta y actualización, y por último el de consulta, actualización y modificación de la información (artículo 7, inciso a).

4. La seguridad del sistema y el derecho a la intimidad del paciente

En este contexto es preciso recordar el artículo 2 de la ley de derecho de los pacientes que en su inciso c) establece, en cuanto al derecho personalísimo a la intimidad del paciente, que: "Toda actividad médico-asistencial tendiente a obtener, clasificar, utilizar, administrar, custodiar y transmitir información y documentación clínica del paciente debe observar el estricto respeto por la dignidad humana y la autonomía de la voluntad, así como el debido resguardo de la intimidad del mismo y la confidencialidad de sus datos sensibles, sin perjuicio de las previsiones contenidas en la ley 25.326".

A su vez, el inciso d) pone énfasis en el derecho a la confidencialidad: "El paciente tiene derecho a que toda persona que participe en la elaboración o manipulación de la documentación clínica, o bien tenga acceso al contenido de la misma, guarde la debida reserva, salvo expresa disposición en contrario emanada de autoridad judicial competente o autorización del propio paciente".

El derecho a la intimidad del paciente, en mi opinión, es uno de los derechos menos respetados a pesar de ser el que mayor importancia tiene en la relación médico paciente, después de los derechos a la vida y a la salud. Es que la vida privada de la persona se expone, casi naturalmente en el ámbito de la salud y, por tanto, no puede quedar expuesta a terceros. Se trata de derechos protegidos por la Constitución Nacional en el artículo 19, que asegura la privacidad, y en el artículo 43, que protege los datos personales mediante la garantía del *habeas data*.

La Corte Europea de Derechos Humanos ha dado una noción amplia del derecho a la intimidad, cuando afirmó que "el respeto por la vida privada también debe abarcar, en cierta medida, el derecho del individuo a establecer y desarrollar relaciones con sus semejantes", y considera que "cada uno tiene el derecho a vivir como desea y el derecho a ser percibido como uno es"[7].

El Código Civil y Comercial de la Nación no regula el derecho a la intimidad en el Libro Primero, Título 1, Capítulo 3. Allí, después de aludir en el artículo 51 a la dignidad de la persona, en el artículo 52 prevé la consecuencia que se deriva de la lesión a la intimidad de la persona humana*, a su* "honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme a lo dispuesto en el Libro Tercero, Título V, Capítulo 1". Precisamente, es en el capítulo mencionado, en el artículo 1770, donde se incluye una noción de derecho a la intimidad: "El que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo con las circunstancias…".

El derecho a la intimidad incluye el derecho a los datos personales, es decir, la facultad de la persona para controlar la recolección y el tratamiento de los datos personales. Estos derechos personalísimos son los que pueden quedar expuestos en la HC y, mucho más, en la HCE.

No hay duda acerca de que la vida privada en la actualidad está expuesta de manera notoria, pues la tecnología facilita todos los medios para la intromisión arbitraria en la intimidad, desde un *hacker* que viola la información de un medio de salud hasta cualquier personal de salud que, sin derecho, vulnera la información de los pacientes.

Respecto de la intromisión en las HC de los pacientes preocupa porque la intromisión y la perturbación de la intimidad se produce, por lo general, por el manejo de sus datos sensibles[8]. Son múltiples los modos de invadir esa privacidad tan respetada y cuidada, en lo formal, pero muy desprotegida en la realidad.

En protección de ese derecho debe encargarse a los técnicos la mayor perfección en los aspectos tecnológicos y la interoperabilidad del sistema porque así lo exige la seguridad del registro que se propone.

En el Capítulo II, al regular el Sistema único se establecen las pautas concretas que tienden a lograr su seguridad. El artículo 6 señala como carácter distintivo del sistema la confidencialidad de la información que alberga. Los responsables de la administración y el resguardo de dichos datos serán designados por la autoridad nacional y deberán actuar sujetos a la responsabilidad administrativa, civil o penal. Esta norma debe ser concordada con el artículo 21 de la ley 26.529: "Sanciones. Sin perjuicio de la responsabilidad penal o civil que pudiere corresponder, los incumplimientos de las obligaciones emergentes de la presente ley por parte de los profesionales y responsables de los establecimientos asistenciales constituirán falta grave, siendo pasibles en la jurisdicción nacional de las sanciones previstas en el tít. VIII de la ley 17.132 –Régimen Legal del Ejercicio de la Medicina, Odontología y Actividades Auxiliares de las mismas– y, en las jurisdicciones locales, serán pasibles de las sanciones de similar tenor que se correspondan con el régimen legal del ejercicio de la medicina que rija en cada una de ellas".

La confidencialidad que se exige y que la ley consigna en forma expresa debe ser procurada con elementos técnicos que impidan el acceso y la difusión de la información extremadamente sensible que el Registro conservará. A esos fines, el inciso b) del artículo que comentamos dispone que el registro de la información, su actualización o modificación y consulta se efectúan en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad, acceso y trazabilidad. Desde antes, ya la ley 26.529 preveía la seguridad de la HCE: "A tal fin, debe adoptarse el uso de accesos restringidos con claves de identificación, medios no reescribibles de almacenamiento, control de modificación de campos o cualquier otra técnica idónea para asegurar su integridad".

El referido artículo 6 enuncia en el inciso b) los caracteres que debe reunir la información: seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad, acceso y trazabilidad. Luego, en el artículo 7 el legislador explica la noción que tiene de algunas de esas voces. Por ejemplo, trazabilidad la explica como: cualidad que permite que todas las acciones realizadas sobre la información y/o sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad, dejando rastro del respectivo acceso. Dada la fragilidad de los datos que contiene este Registro, el legislador, siguiendo las indicaciones de las normas argentinas y del derecho comparado, insiste en exigir todos aquellos resguardos que aseguren su intangibilidad.

Será un adelanto significativo el libre acceso y seguimiento de la HC por parte del paciente. Garantizar el seguimiento implica que, en cualquier momento y desde cualquier lugar del país, el paciente puede acceder al Registro y verificar quienes han intentado o han entrado al contenido de sus datos clínicos, si son personas autenticadas o no, y puede averiguar las razones de esas consultas. Como se advierte, esto facilita la inmediatez del acceso del paciente a su HC y viene a resolver el problema que se ha planteado recurrentemente desde hace años, por la falta de entrega de esa historia a requerimiento de los pacientes que los obliga a ocurrir a la vía judicial. La resistencia a la entrega de la HC trata de ocultar, en la mayoría de los casos, un problema mayor[9] que es la mala confección del docu-

(7) Canas, S., Conseiller référendaire à la Cour de cassation, "L'influence de la fondamentalisation du droit au respect de la vie privée sur la mise en oeuvre de l'article 9 du code civil", en Nouveaux Cahiers du Conseil constitutionnel N° 48 (Dossier : vie privée), juin 2015, pp. 47 - 58.

(8) Por ejemplo, en CNTrab. Sala II, 21/04/2022, "Leccadito, Andrea Verónica c. Socorro Médico Privado S.A. s/ despido" [DT 2022 (julio), 140, RDLSS 2022-21, 30], se sancionó la publicación de datos de salud por parte de un empleado en una red social; C. Civ. y Com. Córdoba, n° 5, 10/06/2008, "F., M. I. v. B., H. y otros", (TR LALEY 70046212), se denegó el secuestro de historias clínicas si no se tenía el consentimiento de los pacientes que eran sus titulares.

(9) Por ejemplo, en CNCiv., Sala F, 11/08/2022, "N., P. G. c. Centro de Ojos Buenos Aires y otro s/ Habeas data" (La Ley 20/09/2022, 10, TR LALEY AR/JUR/103661/2022), se hace lugar al *habeas data* por falta de entrega de la historia clínica; en SCBuenosAires, 06/11/2019, "Suelgaray, Guillermo Hugo c. Rivas, Horacio y

mento y la falta de seguridad que padecen en la actualidad estos documentos, que constituyen una parte fundamental de los derechos personalísimos del paciente y, sin embargo, permanecen a disposición solo del equipo médico, y, por tanto, son pasibles de las más diversas alteraciones.

Vinculado con las cuestiones judiciales, que por lo general se refieren a la mala praxis, la ley dispone, como hemos visto, que la información contenida en el Sistema Único de Registro de Historias Clínicas Electrónicas constituye documentación auténtica y, como tal, es válida y admisible como medio probatorio, haciendo plena fe a todos los efectos, siempre que se encuentre autenticada.

Con el fin de garantizar aún más la confidencialidad de la información, la ley o su reglamentación deberían disponer, de manera expresa, que:

a) La información no puede ser revelada a terceros sin el consentimiento del titular, ni intencionada ni accidentalmente, salvo casos excepcionales y autorización judicial. La nueva ley exige que el sistema sea auditable y pasible de ser inspeccionado por las autoridades correspondientes por lo que se crea una situación problemática ante la difusión de datos. Entendemos que cualquier auditoría solo será posible si la información obrante en las HCE ha sido anonimizada en forma correcta, pues, en caso contrario la privacidad del paciente está expuesta a su vulneración.

b) Que los datos de la HC no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Esta prohibición está vinculada a la interpretación restrictiva del consentimiento del paciente. Por ejemplo, no podría emplearse la información registrada con fines de investigación médica si cada uno de los pacientes, titulares de las HCE, no ha prestado su consentimiento expreso a tal fin.

5. Los profesionales obligados

Como se advierte con la lectura de la ley, su finalidad es lograr la informatización completa del sistema en un proceso que, sin duda, demandará su tiempo. Aun así, es importante determinar quiénes son las personas vinculadas con el sistema de salud que están alcanzadas por esta normativa, en especial, es importante saber en qué situación se encuentran los profesionales que ejercen de manera privada por fuera de los efectores públicos o privados.

La ley de derechos del paciente tampoco tiene una norma al respecto, pero su decreto reglamentario establece en el artículo 12 que: "Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y custodia de la documentación asistencial que generen".

La nueva ley parece comprender a todos los profesionales, pero no lo aclara, dice en el artículo 3 que "toda intervención médico-sanitaria a cargo de profesionales y auxiliares de la salud, que se brinde en el territorio nacional, ya sea en establecimientos públicos del sistema de salud de jurisdicción nacional, provincial o municipal, y de la Ciudad Autónoma de Buenos Aires, como en establecimientos privados y de la seguridad social". Además, el artículo 6, inciso c), tiene una extensión similar cuando exige que se garanticen los mecanismos informáticos para la autenticación de las personas, agentes, profesionales y auxiliares de la salud que intervengan en el Sistema Único de Registro de Historias Clínicas Electrónicas.

Esta falta de precisión deberá subsanarse, pues, para los profesionales que ejercen de manera individual y privada no será un trámite sencillo adherir al Sistema registral de las HCE.

Por otro lado, sería conveniente prever que el *software* y las cuestiones técnicas, en general, sean probados con el personal sanitario que lo usará, a fin de evitar que las complejidades de la tecnología fomenten el rechazo al sistema como sucedió, por ejemplo, en Francia que tuvo resistencia por parte de los médicos, quienes consideraron que no resultaba adecuado a su trabajo[10].

Se requiere también la armonización del vocabulario técnico informático. Con seguridad habrá que pulir la cuestión en relación a los términos médicos en la reglamentación. Esa necesidad de armonización parecería que en parte está satisfecha en nuestra ley de derechos del paciente porque el artículo 15 exige que los registros de los actos realizados por los profesionales y auxiliares intervinientes; los antecedentes genéticos, fisiológicos y patológicos del paciente, si los hubiere; las historias clínicas odontológicas, y todo acto médico deben ser realizados sobre la base de nomenclaturas y modelos universales adoptados y actualizados por la Organización Mundial de la Salud (OMS), todo lo cual debe ser confeccionado, según el decreto reglamentario sobre la base de nomenclaturas CIE 10 de la OMS, o las que en el futuro determine la autoridad de aplicación.

6. La experiencia en otros países

Nuestro país se sumará pacientemente a los países que han implementado sistemas digitalizados. Será un largo proceso que, como se vio, viene retrasándose desde hace años. La única ventaja de nuestro letargo es que podremos abrevar en las experiencias internacionales.

Desde un punto de vista de la política de salud pública general de la Unión Europea se observa la preocupación por la digitalización y su seguridad. Se está propiciando el intercambio transfronterizo de datos de las HC, denominadas en ese ámbito "historiales médicos electrónicos". Han considerado que es un derecho de los ciudadanos de la Unión acceder a las bases de datos, en especial, los datos sanitarios, sin embargo, no están pudiendo hacerlo a través de las fronteras, lo cual es perjudicial sobre todo cuando el movimiento transfronterizo de personas y familias es creciente.

La Comisión de la UE dictó el 6 de febrero de 2019 la recomendación (UE) 2019/243 sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo. Se establece un marco general que consta de: a) un conjunto de principios que regulen el acceso a historiales médicos electrónicos y el intercambio de esos historiales a través de las fronteras; b) un conjunto de especificaciones técnicas comunes para el intercambio transfronterizo de datos en determinados dominios de información sanitaria. Sería la base de referencia para un formato de intercambio de historiales médicos electrónicos de ámbito europeo; c) un proceso para avanzar en el desarrollo de ese formato.

Más recientemente, en diciembre de 2022, se dictó la 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, en cuyo texto se incluyen las metas digitales hasta 2030, entre ellas, la digitalización de los servicios públicos que fija la pauta del 100% de los ciudadanos de la Unión con acceso a sus historiales médicos electrónicos.

En setiembre de 2022, se informa acerca de un avance de la comunidad europea al ofrecerse el Espacio Europeo de Datos de Salud (EEDS), que se basa en dos infraestructuras transfronterizas: MyHealth@EU, y HealthData@EU. Los servicios de MyHealth@EU ofrecen la posibilidad de emitir recetas electrónicas y contiene el perfil sanitario sintético de los ciudadanos. Este servicio ya está disponible en 10 países europeos[11]. Este servicio permite a los profesionales de la salud acceder a información esencial (más allá de las fronteras). HealthData@EU facilita el acceso a la información sanitaria electrónica para usos secundarios, como la investigación, la innovación o la elaboración de políticas. Esto ofrece la oportunidad de aprovechar un enorme catálogo de datos sanitarios. Se trata de sistemas en los que se puede acceder a la información de los pacientes bajo altas medidas estándares de seguridad y privacidad.

En 2006, España decidió abordar el Proyecto de Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS) para dar una respuesta realista y en un plazo razonable a una necesidad de la salud pública y de la población que había sido bien identificada.

---

otros s/ daños y perjuicios" (La Ley Online; C.122.323, TR LALEY AR/JUR/45765/2019), se sanciona la carencia de historia clínica original, y en CNCiv., Sala I, 05/08/2020, "P. N. V. c. La Obra Social del Papel Cartón y otros s/ daños y perjuicios" (La Ley Online; TR LALEY AR/JUR/35374/2020), se imputa incumplimiento de las recomendaciones médicas ante las severas deficiencias en la HC.

(10) Morquin, D., *Comment améliorer l'usage du Dossier Patient Informatisé dans un hôpital? Vers une formalisation habilitante du travail intégrant l'usage du système d'information dans une bureaucratie professionnelle. Gestion et management,* Université Montpellier, 2019, Français, NNT:2019MONTD005, especialmente puede verse, p. 122.

(11) Según la página *web*: European Commision, "Salud pública" https://health-ec-europa-eu.translate.goog/other-pages/basic-page/myhealtheu-flyer-addressed-patients-and-health-professionals_en?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc (fecha de consulta 07/04/2023). Al 7 de abril de 2023 la casi totalidad de los países de la UE ofrecen el sistema.

De entrada, se tuvo en consideración que, a la hora de abordar un sistema con las características y objetivos planteados, resultaba imprescindible mantener equilibrados, en el nivel más alto posible, dos valores: la disponibilidad de la información para el ciudadano y los profesionales que deban prestarle atención sanitaria y la protección de su intimidad, en relación con los datos que afectan a su salud. Dos cuestiones que nuestra nueva ley ha considerado reiteradamente.

Un principio básico es que ningún profesional que deba asistir al paciente tenga dificultades para acceder al sistema y que el ciudadano tenga disponibilidad. El primero deriva del principio de beneficencia, y el segundo, del principio de autonomía. Por supuesto, ninguno de ellos debe supeditarse al otro y ambos deben ser preservados por igual en el mayor nivel posible.

Además, se tuvo en cuenta que debía adoptarse un vocabulario sanitario controlado y estandarizado que permitiera la interpretación inequívoca y automática de los contenidos transmitidos entre sistemas distintos de forma precisa y en idiomas diferentes, a fin de facilitar el acceso a la información relevante para la toma de decisiones clínicas.

Se crea un sistema de seguimiento sistemático de los accesos a cargo de un Consejo de Administradores del sistema, sin duda es una garantía importante si ese Consejo trabaja de manera sostenida y eficiente.

En Francia, el acceso a la información del paciente está regulado por la ley a partir de la Ley Nº 2002-303 sobre derechos de los pacientes. El paciente tiene derecho a acceder a la información sobre su salud ya sea que se encuentre en manos de efectores de salud o de profesionales. Los agentes y efectores de salud tienen autonomía para implementar los programas informáticos. Para fomentar la informatización hay controles asiduos y programas de financiamiento. Entre ellos, en 2019 se dictó la instrucción DGOS/PF5/2019/32 que constituye el lanzamiento operacional del Programa HOP'EN que tiene por finalidad lograr lo que denominan Hospital numérico abierto a su entorno. Cuenta con importante financiamiento que se otorga después de analizar el estado de desarrollo que cada efector tenga en relación con la Historia clínica informatizada (*Dossier Patient Informatisé* –DPI–) y también a la Historia clínica resumida (*Dossier Médical Partagé* –DMP–), que contiene algunos datos seguros en línea y es una parte de la HC del paciente.

7. Conclusión

La ley que analizamos de manera preliminar significa un buen paso en la senda de la mejora en la atención de la salud, pero obliga a garantizar la mayor eficiencia en la protección de la privacidad de las personas titulares de las HCE.

VOCES: HISTORIA CLÍNICA - PROTECCIÓN DE DATOS PERSONALES - TECNOLOGÍA - PERSONA - CONSTITUCIÓN NACIONAL - INTIMIDAD - DERECHOS Y GARANTÍAS CONSTITUCIONALES - INFORMÁTICA - INTELIGENCIA ARTIFICIAL - DERECHOS PERSONALÍSIMOS - ORDEN PÚBLICO - HÁBEAS DATA - DERECHOS HUMANOS - SECRETO PROFESIONAL - DAÑOS Y PERJUICIOS - DAÑO MORAL - DAÑO PSÍQUICO - RESPONSABILIDAD CIVIL - MÉDICO - MEDICAMENTOS - CONTRATOS - OBLIGACIONES - CÓDIGO CIVIL Y COMERCIAL - ACTOS Y HECHOS JURÍDICOS - COMERCIO E INDUSTRIA - POLÍTICAS PÚBLICAS - SALUD PÚBLICA - CONSENTIMIENTO - PRUEBA - CARGA DE LA PRUEBA - HOSPITALES Y SANATORIOS - MÉDICO - OBRAS SOCIALES - DERECHOS DEL CONSUMIDOR - MEDICINA PREPAGA - PROFESIONALES DE LA SALUD

El Programa Federal Único de Informatización y Digitalización de las Historias Clínicas a la luz de la obligación de seguridad de los datos

por Verónica Elvia Melo(*)

Introducción

Mediante la ley 27.706, se creó el Programa Federal Único de Informatización y Digitalización de las Historias Clínicas en la República Argentina, circunstancia que entraña numerosas ventajas a los médicos y pacientes, así como al sistema de salud en general. No obstante, las preocupaciones acerca de la seguridad y la privacidad relacionadas con la información de los pacientes podrían demorar la implementación de las historias clínicas electrónicas. Preservar la ingente cantidad de datos sensibles acerca de la salud de los pacientes en diferentes formularios (digitales) se erige en el gran desafío de esta modalidad de historias clínicas.

Con anterioridad, la ley 14.494 de la provincia de Buenos Aires reguló el sistema de historia clínica electrónica y sentó dos parámetros sumamente relevantes en la temática. Por un lado, el principio de confidencialidad, que obliga a tratar los datos relativos a la salud de la persona con la más absoluta reserva (artículo 8 de la Ley 14.494). Y, por el otro, el principio de accesibilidad restringida, según el cual el titular de los datos consignados en la his-

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *La indemnización correspondiente por la no obtención del consentimiento informado en la praxis médica*, por Roberto A. Vázquez Ferreyra, ED, 197-709; *Historia clínica. Encuadre probatorio. Responsabilidad médica. Responsabilidad omisiva*, por Lucía Graciela Savarese, ED, 216-642; *El derecho a la salud como derecho social. Garantía de la dignidad del hombre*, por Violeta Castelli, EDA, 2007-743; *El plazo de la prescripción liberatoria en materia de responsabilidad médica en los hospitales de la Ciudad Autónoma de Buenos Aires*, por Inés Amura, Esteban Centanaro y Juan Pablo Rodríguez, ED, 234-708; *Responsabilidad médica por mala praxis*, por Mariano Gagliardo, ED, 251-465; *Los médicos y el consentimiento informado (Necesarias precisiones sobre el tema en el marco del nuevo CCC)*, por Marcelo J. López Mesa, ED, 266-703; *La doctrina de la "real malicia" y el derecho a la información sobre cuestiones médicas*, por María Angélica Gelli, ED, 277; *Consentimiento informado de las personas con discapacidad en tratamientos médicos*, por Nicolás Pildayn y Marina M. Sorgi Rosenthal, ED, 279; *La protección de los datos personales en internet (una tarea ineludible)*, por Esteban Ruiz Martínez, ED, 284-726; *Datos personales: Google se asocia con el sistema de salud más importante de Estados Unidos*, por Laura Belén Yachelini, ED, 286-618; *El médico y la virtud de la prudencia en tiempos de pandemia*, por Germán Calabrese, ED, 289-1581; *Odontólogos. Responsabilidad civil profesional en tiempos de pandemia*, por Dante Gómez Haiss, 289-1434; *La responsabilidad del médico especialista*, por Milton H. Kees, ED, 290; *La regulación del derecho a la imagen y el régimen de protección de datos de carácter personal. Ciertas "fricciones" entre ambos regímenes*, por Guillermo F. Peyrano, ED, 290-637; *Responsabilidad del médico: necesidad de deslindar el casus de la no culpa*, por Federico Ossola y Julieta Bollero Hauser, ED, 291; *El derecho a la información de salud y el hábeas data específico*, por Eduardo Molina Quiroga, ED, 294; *Derecho a la intimidad de los datos de salud*, por Julián Prieto, ED, 300. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Abogada (UCA). Magíster en Asesoramiento Jurídico de Empresas (Universidad Austral). Especialista en Derecho de Alta Tecnología (UCA). Doctora en Derecho (Universidad Nacional de Rosario). Profesora titular ordinaria (UCA Campus Rosario). Directora de la Carrera de Especialización en Derecho de Daños (UCA Campus Rosario).

toria clínica electrónica tendrá en todo momento derecho a conocerlos (artículo 10 de la Ley 14.494).

En cuanto a la legislación nacional, se encuentran vigentes varias normas relativas a las historias clínicas y los datos obrantes en ellas, con especial referencia a los derechos del paciente titular de dichos datos. Por ejemplo, la ley 26.529 estatuye que el paciente tiene derecho a que toda persona que participe en la elaboración o manipulación de la documentación clínica, o bien tenga acceso a su contenido, guarde la debida reserva, salvo expresa disposición en contrario emanada de autoridad judicial competente o autorización del propio paciente[1]. A su turno, la ley 23.798, que declara de interés nacional a la lucha contra el síndrome de inmunodeficiencia adquirida, incorpora una prohibición expresa de recolección o almacenamientos de datos que permitan individualizar a los pacientes afectados por dicha enfermedad, los que deberán gestionarse en forma codificada[2]. En otro orden, pero siempre en la línea del respeto de la privacidad y la confidencialidad, la ley 26.378 –que ratifica la Convención sobre los Derechos de las Personas con Discapacidad y su protocolo facultativo– requiere que se asegure la confidencialidad y el respeto de la privacidad en la recopilación y mantenimiento de la información de las personas con discapacidad.

El propósito de este trabajo es identificar estas cuestiones atinentes a la privacidad y a la seguridad, y las posibilidades de gestionarlas.

1. Ideas preliminares

Una historia clínica electrónica puede definirse como la versión electrónica de la historia del paciente en la medida en que es conservada por los prestadores de salud durante un tiempo determinado y comprende todos los datos clínicos relacionados con los tratamientos administrados a dicho paciente por parte de algún prestador del sistema de salud, tales como enfermedades, fármacos prescritos, síntomas, vacunas, datos de laboratorio e informes radiológicos[3]. El artículo 8 de la ley 27.706 define a la historia clínica electrónica en los siguientes términos: "El paciente es titular de los datos y tiene en todo momento derecho a conocer la información en la Historia Clínica Electrónica, que es el documento digital, obligatorio, con marca temporal, individualizada y completa, en el que constan todas las actuaciones de asistencia a la salud efectuadas por profesionales y auxiliares de la salud a cada paciente, refrendadas con la firma digital del responsable […]"[4]. A su vez, la ya referida ley provincial (de Buenos Aires) 14.494 la define como el conjunto de datos clínicos, sociales y administrativos referidos a la salud de una persona, procesados a través de medios informáticos o telemáticos[5].

Con la entrada en vigor de esta ley 27.706, que crea el Programa Federal Único de Informatización y Digitalización de las Historias Clínicas en la República Argentina, la desmaterialización que viene operándose en numerosos ámbitos llega al sistema de salud y se estima que el sistema integrado de historias clínicas electrónicas podría mejorar la prestación del servicio de salud.

Se ha sostenido que las historias clínicas centralizadas son más efectivas en la medida que reducen costos, mejoran la prestación del servicio de salud a la vez que promueven los tratamientos médicos basados en la experiencia y aseguran la portabilidad de las historias clínicas[6]. Sin embargo, en aras de una auténtica efectividad, este Programa Federal Único de Informatización y Digitalización de las Historias Clínicas en la República Argentina debe satisfacer ciertas exigencias, tales como lograr que los datos estén completos, resiliencia frente al error, estar disponibles y ser coherentes con las políticas de seguridad[7].

2. La insoslayable referencia a la ley 25.326 de protección de datos personales

Es sabido que el objeto de la ley 25.326 es la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información registrada[8]. Estos archivos, registros, base o banco de datos refieren al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso[9].

A continuación, es la misma ley la que define el tratamiento de los datos como aquellas operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias[10].

En este sentido, si proyectamos estas definiciones al sistema de historias clínicas electrónicas, se destacan dos aspectos. Por un lado, su naturaleza encuadra en el concepto de base o banco de datos; y, por el otro, toda la información que circula por sus redes se encuentra sujeta a un procedimiento de tratamiento ordenado a que los interesados puedan acceder a la información allí almacenada mediante los campos de búsquedas diseñados al efecto. Por este motivo, entendemos que toda la información almacenada y procesada por este sistema se encuentra tutelada por la ley de protección de datos personales.

Como corolario de lo expuesto, cobra relevancia el concepto de la calidad de los datos almacenados y que la ley se encarga de proteger en el artículo 4º, que formula una serie de principios cuya observancia es irrefragable[11].

(1) "Artículo 2° - Derechos del paciente. Constituyen derechos esenciales en la relación entre el paciente y el o los profesionales de la salud, el o los agentes del seguro de salud, y cualquier efector de que se trate, los siguientes: […] d) Confidencialidad. El paciente tiene derecho a que toda persona que participe en la elaboración o manipulación de la documentación clínica, o bien tenga acceso al contenido de la misma, guarde la debida reserva, salvo expresa disposición en contrario emanada de autoridad judicial competente o autorización del propio paciente […]".

(2) "Artículo 2° - Las disposiciones de la presente ley y de las normas complementarias que se establezcan se interpretarán teniendo presente que en ningún caso pueda: […] e) Individualizar a las personas a través de fichas, registros o almacenamiento de datos, los cuales, a tales efectos, deberán llevarse en forma codificada".

(3) Centers for Medicare & Medicaid Services, "Electronic Health Records", disponible en https://www.cms.gov/Medicare/E-health/EHealthRecords/index.html (fecha de consulta: 5/4/2023).

(4) Ley 27.706, Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina (BO: 16/3/2023).

(5) "Artículo 2. - A los efectos de esta norma se entiende por historia clínica electrónica única; el conjunto de datos clínicos, sociales y administrativos referidos a la salud de una persona, procesados a través de medios informáticos o telemáticos".

(6) Carey, D.; Fetterolf, S.; Davis, F. *et al.* "The Geisinger MyCode community health initiative: an electronic health record–linked biobank for precision medicine research", Genet Med 18, 906-913 (2016), DOI: https://doi.org/10.1038/gim.2015.187.

(7) Allard, T.; Anciaux, N.; Bouganim, L.; Guo, Y.; Le Folgoc, L., Nguyen, B.; Pucheral, P.; Ray, I.; Ray, I.; Yin, S., "Secure personal data servers: a vision paper", PVLDB, 3, 2010.

(8) "Artículo 1°:(Objeto). La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional […]".

(9) "Artículo 2: Definiciones […] Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso […]".

(10) "Artículo 2: Definiciones […] Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias[…]".

(11) "Artículo 4: (Calidad de los datos). 1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. 2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. 4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. 5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley. 6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. 7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados".

Además, los datos que sean total o parcialmente inexactos, o que estén incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la referida ley[12].

Otra noción indispensable a la hora de analizar el régimen del registro de historias clínicas electrónicas es el concepto de dato sensible, ya que se trata de datos especialmente protegidos. Se definen como aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Al abordar la problemática de los datos sensibles, Gozaíni elabora la siguiente taxonomía: a) datos ultrasensibles: los que revelan información de las personas sobre ideología, religión o creencias, cuya recolección o almacenamiento se halla absolutamente prohibida; b) datos especialmente sensibles: los referidos al origen racial, la salud y la vida sexual, que solo se podrían obtener y guardar con expresa autorización del titular; y c) datos sensibles particulares: los que se relacionan con la historia individual de las personas físicas, como los antecedentes penales y contravencionales, que solo pueden ser objeto de tratamiento por las autoridades públicas competentes[13]. Por lo demás, conforme al artículo 7 de la ley 25.326 de protección de datos personales, ninguna persona puede ser obligada a proporcionar información de carácter sensible[14].

Coherentemente con esta tutela reforzada de los datos sensibles, el artículo 9 de la ya referida ley ordena que el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado[15].

3. Breve referencia a la normativa europea. Legislación proyectada

El Reglamento Europeo de Protección de Datos, aprobado en 2016 y vigente desde 2018[16], define a los datos relativos a la salud como "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud"[17]. A su vez, en el considerando 35 del mentado reglamento, se ordena que entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro[18].

De la lectura de la norma reseñada surge la necesidad de conceptualizar con precisión qué se entiende por dato de salud, habida cuenta de las herramientas idóneas para obtener este género de información. En este sentido, Lafferriere se pregunta si un reloj que mide pulsaciones acaso está recogiendo datos de salud, a cuyo respecto debe considerarse que la información que recopilan los dispositivos, como el número de pulsaciones o la tensión arterial, pueden llegar a revelar el estado de salud de una persona y que, por ende, deben catalogarse como datos sensibles[19].

Entre las reformas más significativas que contempla el anteproyecto de actualización de la ley de protección de datos personales[20], impulsado por la Agencia de Información Pública, se encuentra la tutela de los datos sensibles. En efecto, el artículo 17 de la norma proyectada ordena que "en el tratamiento de datos sensibles se debe implementar la responsabilidad reforzada que implica, entre otras características, mayores niveles de seguridad, confidencialidad, restricciones de acceso, uso y circulación. Se prohíbe el tratamiento de datos sensibles, excepto si: a) el Titular de los datos ha dado su consentimiento a dicho tratamiento, salvo en los casos en que por ley no sea requerido el otorgamiento de dicha autorización; b) fuera necesario para salvaguardar el interés vital del Titular de los datos y este se encontrará física o legalmente incapacitado para prestar el consentimiento y sus representantes legales no pudieran realizar en tiempo oportuno; c) es efectuado por establecimientos sanitarios públicos o privados o por profesionales vinculados a la ciencia de la salud con la finalidad de un tratamiento médico específico de acuerdo a lo establecido por la ley 26.529 de Derechos del Paciente, Historia Clínica y Consentimiento Informado y sus modificatorias: se prohíbe a los operadores de planes privados de salud tratar datos de salud para la práctica de selección de riesgo en la contratación de cualquier modalidad y la exclusión de beneficiarios; d) Se realiza en el marco de las actividades legítimas de una fundación, asociación o cualquier otro organismo sin fines de lucro, cuyo objeto principal sea una actividad política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan un contacto regular por razón de su objeto principal, y que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los Titulares; e) se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; f) tuviera una finalidad histórica, de archivo de interés público, de aporte al proceso de memoria, verdad y justicia frente a crímenes de lesa humanidad, estadística o científica; en estos casos y en la medida de lo posible, debe adoptarse, teniendo en cuenta la finalidad, un procedimiento de anonimización o seudonimización; g) fuera necesario para el cumplimiento de obligaciones y el ejer-

(12) "Artículo 16: (Derecho de rectificación, actualización o supresión). 1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos [...]".

(13) Gozaíni, O. A., "La afiliación partidaria como dato sensible que se puede difundir", La Ley 2002-F, 1437, Cita Online: AR/DOC/9318/2001.

(14) "Artículo 7°: (Categoría de datos). 1. Ninguna persona puede ser obligada a proporcionar datos sensibles. 2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. 3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros [...]".

(15) "Artículo 9: (Seguridad de los datos). 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad".

(16) Véase Comisión Europea, "La protección de datos en la UE", disponible en https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es#:~:text=El%20Reglamento%20general%20de%20protecci%C3%B3n%20de%20datos%20(RGPD)&text=Adem%C3%A1s%2C%20la%20existencia%20de%20una,25%20de%20mayo%20de%202018 (fecha de consulta: 25/4/2023).

(17) "Artículo 4: A efectos de este Reglamento se entenderá por: [...] 15) 'datos relativos a la salud': datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud; [...]". El texto del Reglamento Europeo de Protección de Datos está disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:02016R0679-20160504#tocId7 (fecha de consulta: 25/4/2023).

(18) Considerando 35: "Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro", disponible en https://gdpr-text.com/es/read/recital-35/#:~:text=(35)%20Entre%20los%20datos%20personales,mental%20pasado%2C%20presente%20o%20futuro(fecha de consulta: 25/4/2023). En esta transcripción, se han omitido las notas al pie del original.

(19) Lafferriere, J. N., "Los datos personales de salud y su protección jurídica en el ordenamiento jurídico argentino", EBOOK-TR 2023-1 (Gelli), 29, Cita: TR LALEY AR/DOC/541/2023.

(20) Sobre el tema puede verse el editorial: "Principales puntos del proyecto de reforma de la ley de datos personales", 12 de septiembre de 2022, Erreius, disponible en https://www.erreius.com/opinion/14/civil-persona-y-patrimonio/Nota/844/principales-puntos-del-proyecto-de-reforma-de-la-ley-de-datos-personales (fecha de consulta: 25/4/2023).

cicio de derechos específicos del Responsable del tratamiento o del Titular de los datos en el ámbito del derecho laboral y de la seguridad, la salud pública y la protección social; h) sea necesario en ejercicio de las funciones de los poderes del Estado en el cumplimiento estricto de sus competencias. Cuando los organismos públicos traten datos personales sensibles, deben proveer condiciones más estrictas de seguridad, lo que debe implementarse mediante salvaguardas apropiadas adicionales, diseñadas específicamente. i) se realiza en el marco de la asistencia humanitaria"[21].

4. Cuestiones vinculadas a la seguridad y privacidad de las historias clínicas electrónicas

Consideramos que en la especie existen tres prioridades éticas de primer orden, tales son privacidad y confidencialidad, seguridad e integridad y accesibilidad de los datos personales.

4.1. Privacidad y confidencialidad

Es célebre la definición de privacidad que dieran Warren y Brandeis como el derecho a ser dejado en paz[22]. El derecho a la privacidad e intimidad, con fundamento constitucional en el artículo 19 de la CN, protege jurídicamente un ámbito de autonomía individual constituido por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, las preferencias y gustos, las opiniones y creencias sociales y políticas mantenidas en reserva, la salud mental y física y, en suma, las acciones, hechos o datos que, teniendo en cuenta la estimativa social y las formas de vida aceptadas por la comunidad, en un momento dado, están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para esa intimidad[23]. Y así, los datos que se obtienen como consecuencia de una relación médico-paciente son datos sensibles y por eso están protegidos en los artículos 2, 7 y 8 de la ley 25.326 de protección de datos personales.

Uno de los pilares de la protección de la confidencialidad consiste en asegurarse que solamente las personas autorizadas tengan acceso a la información. El proceso de control de acceso comienza con las autorizaciones a los usuarios. Por ejemplo, en un consultorio médico, el administrador debería identificar a los usuarios, determinar a qué nivel de información puede acceder cada uno y asignar nombres de usuarios y contraseñas. Los estándares básicos para las contraseñas incluyen la exigencia de cambiarlas periódicamente, establecer un mínimo de caracteres y la prohibición de repetir contraseñas. Una práctica deseable consiste en establecer una autenticación en dos pasos agregando algún tipo de identificación biométrica.

4.2. Seguridad

La seguridad en este contexto puede definirse como la preservación de la confidencialidad, integridad y disponibilidad de los datos[24]. La creciente preocupación acerca de la seguridad de los datos clínicos de una persona se renueva con las historias clínicas electrónicas, con el uso creciente de *smartphones*, el intercambio de datos instituciones médicas, gobierno, obras sociales y demás actores del ecosistema de salud.

Por otra parte, los datos pueden ser hackeados, manipulados o alterados ya sea por usuarios internos o externos, por tal motivo las medidas de seguridad deben estar orientadas a todo tipo de usuarios. Algunas medidas de protección de estos datos podrían ser *firewalls*, *software* antivirus y *software* para detectar intrusiones o accesos indebidos. Igualmente, aun implementando las mencionadas medidas, parece necesario instaurar algún tipo de programa de seguridad para mantener la integridad de los datos, así como también un sistema de auditorías que permita controlar la trazabilidad de los accesos a estos datos.

En orden a la protección de la seguridad de la información, sería recomendable que los prestadores de servicios de salud que recogen datos para las historias clínicas electrónicas designaran un oficial de seguridad para que elabore un catálogo de usuarios, identifique los riesgos y amenazas al sistema informático, pueda anticipar el nivel de riesgo que pesa sobre la organización y pueda gestionar dichos riesgos de manera eficaz. Otra alternativa consistiría en tercerizar (*outsource*) esta gestión de la seguridad de la información en alguna empresa especializada en el área.

Por su parte, las auditorías de trazabilidad sirven para rastrear toda la actividad del sistema generando marcas de fecha y hora para cada ingreso, listados detallados de la información visualizada, durante cuánto tiempo, quién fue el usuario que accedió a la información, y el ingreso de cualquier modificación a la historia clínica electrónica[25]. Asimismo, los administradores pueden detallar qué informes fueron impresos, qué cantidad de capturas de pantalla se hicieron o incluso la ubicación exacta de la computadora desde la que se envió una solicitud de información. Las alertas frecuentemente se diseñan para disparase ante actividades sospechosas o inusuales, tales como revisar información de un paciente que no se atiende o tratar de acceder a información para la cual no se cuenta con autorización, y así los administradores pueden elaborar informes pormenorizados acerca de cada usuario, grupos de usuarios y las actividades en que se involucraron[26]. Las empresas de *software* están desarrollando programas para automatizar el proceso descripto; así, los usuarios de historias clínicas electrónicas deberían tener presente que, a diferencia de los registros en soporte papel, los accesos a las historias clínicas electrónicas pueden ser rastreados a partir de las credenciales de acceso.

4.3. Integridad y disponibilidad

Toda la información obrante en las historias clínicas electrónicas debe ser fidedigna y debe estar protegida por ciertas garantías tanto técnicas como reglamentarias, enderezadas a generar confianza en todos los operadores del sistema.

La integridad apunta a asegurar que el contenido que se encuentra disponible en una historia clínica electrónica no pueda ser modificado en perjuicio de los usuarios, de modo tal que un momento arroje una información y, en otro instante, otra. En otras palabras, para que estos registros sean fiables no deberían poder ser modificados por ninguno de los usuarios de la plataforma[27]. Naturalmente, nos referimos a las modificaciones irregulares o ilegítimas, es decir, que no responden a la confección de la historia clínica por quien tiene derecho a hacerlo. Esta debilidad de esos sistemas puede ser consecuencia en muchas ocasiones del diseño mismo del sistema de gestión de historias clínicas electrónicas, cuyos amplios permisos de edición del contenido puede dar lugar a este tipo de situaciones.

Por lo demás, la integridad podría verse comprometida debido a errores en la documentación o bien debido a una deficiente integridad de la documentación. Solo a guisa de ejemplo para ilustrar este último supuesto, si al tomar el pulso de un paciente este es de 74 y el responsable de ingresar el dato, por error, ingresa 47, mientras que no hay manera de identificar el error en un sistema manual,

(21) Artículo 17 de la "Propuesta anteproyecto actualización Ley 25.326", de la Agencia de Información Pública, de septiembre de 2022, publicado como Anexo I de la Resolución 119/2022 (BO 12/09/2022). Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/271369/20220912 (fecha de consulta: 27/4/2023).

(22) "The right to be let alone", Warren, S. D.; Brandeis, L. D., "The Right to Privacy", Harvard Law Review 4, no. 5 (1890): 193–220, DOI: https://doi.org/10.2307/1321160.

(23) López Mesa, M., "La protección de la intimidad y la vida privada (Exégesis del art. 1770 del Código Civil y Comercial)", Revista Argentina de Derecho Civil, Número 8 - Agosto 2020, IJ International Group, Fecha: 7/8/2020 - Cita: IJ-CMXXII-911., disponible en https://www.acaderc.org.ar/wp-content/blogs.dir/55/files/sites/55/2020/08/La-protecci%C3%B3n-de-la-intimidad-y-la-vida-privada.pdf (fecha de consulta: 17/4/2023).

(24) Guttman, B.; Roback, E. (1995), "An Introduction to Computer Security: the NIST Handbook, Special Publication (NIST SP)", National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-12r1 (fecha de consulta: 18/4/2023).

(25) AHIMA, "White Paper Identifies Opportunities and Challenges with Collecting, Integrating, and Using Social Determinants of Health Data", 14/2/2023, disponible en https://www.ahima.org/news-publications/press-room-press-releases/2023-press-releases/ahima-white-paper-identifies-opportunities-and-challenges-with-collecting-integrating-and-using-social-determinants-of-health-data/ (fecha de consulta: 19/4/2023).

(26) Harman, L. B.; Flite, C. A.; Bond, K., "Electronic health records: privacy, confidentiality, and security". The virtual mento, VM, *14*(9), 2012, 712–719, DOI: https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209 (fecha de consulta: 19/4/2023).

(27) Ordóñez, C. J., "La gestión y la accesibilidad de la información en los expedientes digitales", elDial.com - DC3066).

la historia clínica electrónica dispone de funciones para alertar que se ingresó un dato anormal[28].

En otro orden, son las propias características de los sistemas de historias clínicas electrónicas las que también pueden comprometer la integridad de los datos contenidos en ellas, como por ejemplo la facilidad con que se puede copiar y pegar contenido, o los menús desplegables (*drop down menus*), que limitan las opciones de diagnóstico de tal modo que el médico no puede ingresar los datos correspondientes a lo que ve en la consulta, sino que debe elegir entre las opciones que le brinda el menú. En la práctica, la necesidad de resolver rápidamente puede conducir a errores[29].

El principio de disponibilidad se refiere a la posibilidad de acceder a los datos aun en escenarios de hackeo de un sistema o de sobrecarga de este, supuestos en que la información contenida se tornaría inutilizable. A fin de asegurar la disponibilidad, los sistemas de historias clínicas electrónicas frecuentemente cuentan con componentes redundantes, denominados sistemas de tolerancia al error, de modo que, si un componente falla o presenta algún inconveniente, el sistema inmediatamente cambiará al componente de respaldo[30].

5. Rasgos propios de los sistemas de seguridad y privacidad de las historias clínicas electrónicas

Las tres aristas para considerar, a la hora de delinear los sistemas de seguridad y privacidad de los registros de historias clínicas electrónicas, son la seguridad física, técnica y administrativa. El aspecto de la seguridad administrativa es la primera salvaguardia que involucra técnicas como llevar adelante auditorías, contar con un oficial de protección de datos, así como disponer de algún plan de contingencia en caso de acaecimiento de algún incidente de seguridad. Sin duda, este aspecto de la seguridad administrativa se enfoca en políticas y procedimientos de *compliance*. El segundo aspecto, el de la seguridad física, se focaliza en proteger la información obrante en estos registros en orden a que tanto *software* como *hardware* no puedan ser accedidos por personas no autorizadas a tal efecto. Así, un ejemplo de medida de seguridad física es la asignación de roles con sus respectivas credenciales de acceso.

La tercera arista, la seguridad técnica, alude a la protección de la totalidad del sistema de información que se encuentra en la red informática de la empresa prestadora de salud. Este tema es crucial a la hora de garantizar la seguridad de los prestadores de salud porque la mayoría de los incidentes de seguridad ocurren vía electrónica a través del uso de computadoras y de dispositivos idóneos para transferir información, como podría ser un puerto USB[31]. La seguridad en su dimensión técnica involucra, por ejemplo, el empleo de *firewalls*, sistemas de criptografía, *software* de antivirus y medidas de autenticación de la información[32].

Estudios de campo en el derecho comparado evidencian que se emplean técnicas combinadas de seguridad para los registros de historias clínicas digitales tales como sistemas de criptografía para la salvaguardia técnica y políticas de educación y empleo de un oficial de protección de datos para garantizar la seguridad en su faz administrativa[33].

Es de vital importancia que estas empresas de salud que cuentan con registros de historias clínicas electrónicas estén pendientes de los adelantos tecnológicos en materia de seguridad a los fines de una adecuada gestión de riesgos.

6. Algunos precedentes judiciales en el derecho comparado

En el proceso de elaboración del presente trabajo no he podido acceder a precedentes domésticos. Sin embargo, la referencia al derecho comparado es enriquecedora, ya que es cuestión de tiempo que tales conflictos se generen entre nosotros.

Entre los antecedentes más interesantes, puede citarse el caso en el que la autoridad de aplicación francesa (CNIL) multó a un médico por la omisión de cumplir con la obligación de seguridad de datos, dado que se podía acceder por medio de la web del médico a las imágenes y datos de sus pacientes[34]**.** La CNIL hizo hincapié en las obligaciones de seguridad del controlador. Tras recordar las disposiciones del artículo 32 del RGPD, la CNIL se remitió a sus propias directrices sobre la seguridad de los datos personales y recomendó el cifrado como medida de seguridad estándar. De manera similar, la Guía práctica para médicos alienta a los médicos a cifrar los datos de sus pacientes con un *software* adecuado. En este caso, la autoridad francesa destacó que ninguno de los datos de libre acceso en Internet estaba encriptado. La CNIL recordó que los registros médicos en cuestión son los denominados datos sensibles en el sentido del artículo 9 del RGPD. Estos datos incluían imágenes médicas, apellidos, nombres y fechas de nacimiento de los pacientes, fechas de exámenes, el nombre de los médicos remitentes y los médicos que realizaron los exámenes, así como el lugar donde se realizó el examen. Los datos estuvieron expuestos durante aproximadamente 4 meses. La CNIL encontró responsable al controlador por no cumplir con sus obligaciones de seguridad en virtud del artículo 32 del RGPD. Según la Autoridad, el controlador tampoco había comunicado la violación de datos de manera oportuna, como lo exige el Artículo 33(1)[35].

Entre los antecedentes italianos, la DPA examinó una violación de datos personales que fue notificada por un responsable del tratamiento, el Hospital Universitario Integrado de Verona, después de que este último, en el curso de sus comprobaciones internas periódicas de privacidad, lo hubiera advertido. La notificación se refería a tres violaciones de datos. El procesamiento no autorizado se refería a datos de salud de empleados que se encontraban en el mismo hospital. En un caso se había accedido con la credencial de un médico que había dejado su escritorio desatendido; en los otros dos casos, un aprendiz y un técnico radiólogo habían ingresado a los registros de salud de sus colegas. En los tres incidentes se constata que el tratamiento no se había realizado para prestar servicios médicos, sino por motivos exclusivamente personales, calificados por el responsable del tratamiento como "mera curiosidad"[36].

La autoridad de aplicación italiana concluyó que la violación de datos podría haberse evitado si el controlador simplemente hubiera observado las pautas de Garante de 2015 sobre el procesamiento de datos de salud de los pacientes que establecen que los derechos de acceso a los datos de salud de los pacientes deben limitarse o minimizarse solo al personal de salud que interviene en el proceso de tratamiento médico de los pacientes y hubiera prestado más atención en el diseño de los perfiles de autorización y capacitación de personal calificado (privacidad por diseño y por defecto). En consecuencia, sobre la base del artículo 83 (5) (a) GDPR, el hospital fue multado con el pago de una multa de EUR 30.000,00 por violación del artículo 5 (1) (f) GDPR. Se han adoptado medidas correctoras, según el artículo 58, apartado 2, letra d) del RGPD, que obligan al responsable del tratamiento a completar la implementación de las medidas técnicas y organizativas pertinentes en relación con la autorización de acceso y los perfiles de acceso a los datos de salud del paciente[37].

El tema reviste una importancia para quienes financian al sistema de salud, en especial las obras sociales y las

(28) Harman, L. B.; Flite, C. A.; Bond, K., "Electronic health records: privacy, confidentiality, and security", ya citado.

(29) AHIMA, "Auditing Copy and Paste", Journal of AHIMA 80, no.1 (January 2009): 26-29, disponible en https://library.ahima.org/doc?oid=87789Article (fecha de consulta: 20/4/2023)

(30) Harman, L. B.; Flite, C. A.; Bond, K. "Electronic health records: privacy, confidentiality, and security", ya citado.

(31) Liu, V.; Musen, M.A.; Chou T.; "Data breaches of protected health information in the United States". JAMA. 2015 Apr 14;313(14):1471-3, DOI: 10.1001/jama.2015.2252. Erratum in: JAMA. 2015, Jun 23-30;313(24):2497. PMID: 25871675; PMCID: PMC4479128 (fecha de consulta: 24/4/2023).

(32) Kruse, C.S.; Smith, B.; Vanderlinden, H. *et al.*, "Security Techniques for the Electronic Health Records". J Med Syst 41, 127, 2017, DOI: https://doi.org/10.1007/s10916-017-0778-4 (fecha de consulta: 24/4/2023).

(33) Keshta, I., Odeh, A. "Security and privacy of electronic health records: Concerns and challenges", Egyptian Informatics Journal, Volume 22, Issue 2, 2021, págs. 177-183, ISSN 1110-8665, DOI: https://doi.org/10.1016/j.eij.2020.07.003.(https://www.sciencedirect.com/science/article/pii/S1110866520301365) (fecha de consulta: 24/4/2023).

(34) Véase CNIL - SAN-2020-014, disponible en https://gdprhub.eu/CNIL_-_SAN-2020-014 (fecha de consulta: 25/4/2023).

(35) Ídem.

(36) "Garante per la protezione dei dati personali -9269629", disponible en https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_-_9269629 (fecha de consulta: 25/4/2023)

(37) Ídem.

empresas de medicina prepaga, así como también para las empresas de tecnología que gestionan datos médicos e historias clínicas electrónicas.

Conclusiones

La creación de registros unificados de historias clínicas electrónicas permite compartir la información médica entre los diferentes interesados, y se puede acceder y actualizar la información sobre el paciente al tiempo que este recibe los diversos tratamientos médicos. En este contexto, la seguridad y la privacidad devienen en preocupaciones de primer orden.

Lo cierto es que la medicina se ha vuelto progresivamente cada vez más basada en datos y las tecnologías de la información pueden respaldar los procesos de toma de decisiones de los médicos con herramientas informáticas que funcionan en base a datos e información. En un punto resultará indispensable que tanto el médico como todo el *staff* sanitario puedan confiar en los datos para el cuidado del paciente y para la toma de decisiones. Por ese motivo, la unificación de las historias clínicas electrónicas reclama el conocimiento experto tanto del médico como de los profesionales de la tecnología y del manejo de la información.

VOCES: HISTORIA CLÍNICA - PROTECCIÓN DE DATOS PERSONALES - TECNOLOGÍA - PERSONA - CONSTITUCIÓN NACIONAL - INTIMIDAD - DERECHOS Y GARANTÍAS CONSTITUCIONALES - INFORMÁTICA - INTELIGENCIA ARTIFICIAL - DERECHOS PERSONALÍSIMOS - ORDEN PÚBLICO - HÁBEAS DATA - DERECHOS HUMANOS - SECRETO PROFESIONAL - DAÑOS Y PERJUICIOS - DAÑO MORAL - DAÑO PSÍQUICO - RESPONSABILIDAD CIVIL - MÉDICO - MEDICAMENTOS - CONTRATOS - OBLIGACIONES - CÓDIGO CIVIL Y COMERCIAL - ACTOS Y HECHOS JURÍDICOS - COMERCIO E INDUSTRIA - POLÍTICAS PÚBLICAS - SALUD PÚBLICA - CONSENTIMIENTO - PRUEBA - CARGA DE LA PRUEBA - HOSPITALES Y SANATORIOS - OBRAS SOCIALES - DERECHOS DEL CONSUMIDOR - MEDICINA PREPAGA - PROFESIONALES DE LA SALUD

Claroscuro digital: el Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina. Interoperabilidad. Protección de datos personales

por Matilde Pérez(*)

Sumario: I. Introducción. – II. Primer claroscuro. La Historia Clínica Electrónica (HCE). La interoperabilidad. – III. Segundo claroscuro. El consentimiento informado del paciente. – IV. Tercer claroscuro. Vulnerabilidad en la protección de datos personales. – V. Compás de espera. Reglamentación.

I. Introducción

Con el dictado de la ley 27.706 se crea el "Programa Federal de Informatización y Digitalización de las Historias Clínicas" en nuestro país, en el marco del proceso de implementación de la historia clínica electrónica en el sistema de salud.

El derecho a la salud, como aspiración constitucional, requiere de un sistema coordinado que permita que ciudadanos (pacientes, profesionales de la salud, consumidores) así como a los diversos prestadores (instituciones sanitarias, farmacéuticas, laboratorios) puedan ser usuarios del Programa. Su puesta en marcha permitiría vertebrar la conformación, portabilidad y confiabilidad de los diversos actos de salud plasmados en las historias clínicas y facilitar así la interoperabilidad.

De ese modo, se busca integrarse en los modelos de gestión de sistema único de Historias Clínicas a la manera del modelo islandés adaptado y adoptado en el ámbito europeo o en algunos estados de Estados Unidos de América. En nuestro país, además, el Programa se integra como un plexo normativo junto con las leyes 26.529, 25.326 y 25.506 referidas a la historia clínica digital, la protección de datos personales, así como la firma digital.

Se persigue la integración federal de las historias clínicas para lograr la interoperabilidad de sistemas e informaciones en toda la extensión del territorio y común al sistema de salud público, privado y de seguridad social, con una autoridad central que garantice estrictas medidas de seguridad y transparencia.

Sin embargo, una primera lectura de su texto pone en relevancia diversos claroscuros sobre la oportunidad y el contenido de la norma.

El Capítulo I debe ser analizado desde la perspectiva constitucional y administrativa con relación al reparto de competencias en salud entre Nación, provincias, municipios, sistema privado y seguridad social, ante la imposición de un Sistema Único de carácter federal.

En lo que hace a la organización administrativa del Programa, delega en el Poder Ejecutivo la designación de la autoridad nacional (federal) de aplicación (art. 2) y establece sus atribuciones (competencias), aunque con un margen de discrecionalidad en la reglamentación al indicar que "tiene, entre otras," las facultades allí enumeradas. Esto es, el Poder Ejecutivo puede ampliar las competencias de la futura autoridad de aplicación.

En esta línea, delega también en el Poder Ejecutivo la forma de coordinación de los recursos, así como el plazo para poner en marcha el sistema y la convivencia entre los sistemas de soporte papel y electrónico[1].

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *La indemnización correspondiente por la no obtención del consentimiento informado en la praxis médica*, por Roberto A. Vázquez Ferreyra, ED, 197-709; *Historia clínica. Encuadre probatorio. Responsabilidad médica. Responsabilidad omisiva*, por Lucía Graciela Savarese, ED, 216-642; *El derecho a la salud como derecho social. Garantía de la dignidad del hombre*, por Violeta Castelli, EDA, 2007-743; *El plazo de la prescripción liberatoria en materia de responsabilidad médica en los hospitales de la Ciudad Autónoma de Buenos Aires*, por Inés Amura, Esteban Centanaro y Juan Pablo Rodríguez, ED, 234-708; *Responsabilidad médica por mala praxis*, por Mariano Gagliardo, ED, 251-465; *Los médicos y el consentimiento informado (Necesarias precisiones sobre el tema en el marco del nuevo CCC)*, por Marcelo J. López Mesa, ED, 266-703; *La doctrina de la "real malicia" y el derecho a la información sobre cuestiones médicas*, por María Angélica Gelli, ED, 277-47; *Consentimiento informado de las personas con discapacidad en tratamientos médicos*, por Nicolás Pildayn y Marina M. Sorgi Rosenthal, ED, 279-726; *La protección de los datos personales en internet (una tarea ineludible)*, por Esteban Ruiz Martínez, ED, 284-726; *Datos personales: Google se asocia con el sistema de salud más importante de Estados Unidos*, por Laura Belén Yachelini, ED, 286-618; *El médico y la virtud de la prudencia en tiempos de pandemia*, por Germán Calabrese, ED, 289-1581; *Odontólogos. Responsabilidad civil profesional en tiempos de pandemia*, por Dante Gómez Haiss, 289-1434; *La responsabilidad del médico especialista*, por Milton H. Kees, ED, 290-809; *La regulación del derecho a la imagen y el régimen de protección de datos de carácter personal. Ciertas "fricciones" entre ambos regímenes*, por Guillermo F. Peyrano, ED, 290-637; *Responsabilidad del médico: necesidad de deslindar el casus de la no culpa*, por Federico Ossola y Julieta Bollero Hauser, ED, 291-514; *El derecho a la información de salud y el hábeas data específico*, por Eduardo Molina Quiroga, ED, 294-972; *Derecho a la intimidad de los datos de salud*, por Julián Prieto, ED, 300. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Abogada (UCA). Doctora en Ciencias Jurídicas (UCA). Especialista en Derecho Administrativo (UNLP). Especialista en Entornos Virtuales de Aprendizaje (UCA). Profesora protitular de las asignaturas Obligaciones Civiles y Comerciales, Derecho de Daños y Derechos Reales Parte General y Parte Especial. Profesora invitada en la Maestría de Derecho Civil Patrimonial (UCA). Autora de diversos artículos de doctrina y ponente en Congresos y Jornadas. Miembro de la Comisión de Abogacía Digital de la Facultad de Derecho (UCA).

(1) Se separa de la línea de algunos de los Proyectos presentados en la Cámara de Diputados. Así, el presentado por la diputada Najul preveía en su artículo 6 un plazo máximo de tres años a partir de la

El Capítulo II se ocupa de la conformación de este Sistema Único de Registro y es el eje de este trabajo. Una luz ámbar de atención sobre los alcances de la creación de un banco de datos de salud bajo la órbita de la autoridad nacional de aplicación, de carácter coactivo, en el que se veda al paciente la posibilidad de rechazar ser parte del sistema y sin requerírsele consentimiento informado al respecto. La preocupación se extiende al Capítulo III sobre el tratamiento de datos en materia de Historia Clínica ante una ley como la de Protección de los Datos Personales (ley 25.326) que requiere una urgente actualización.

Es de esperar que su reglamentación por el Poder Ejecutivo en el plazo de 90 días (art. 10) y la puesta en marcha de la autoridad de aplicación (para los que no hay plazo fijado de constitución) subsane estas ausencias, al menos en cuanto sea posible, y contribuya al fortalecimiento de la acabada protección de los pacientes condenados a peregrinar en el laberinto burocrático del sistema de salud.

Este compás de espera en el dictado de la reglamentación y puesta en marcha del Programa no es óbice para el abordaje de algunos claroscuros de la norma: a) la problemática de la interoperabilidad dentro de un sistema federal; b) el consentimiento informado del paciente; c) vulnerabilidad en la protección de datos personales; d) incógnitas de la reglamentación.

II. Primer claroscuro. La Historia Clínica Electrónica (HCE). La interoperabilidad

Los diversos sistemas de información sanitaria (SIS) se organizan en estructuras en las que convergen datos personales e informaciones diversas sobre la salud de las personas a fin a optimizar los procesos de tomas de decisiones para una gestión más eficiente y eficaz de los diversos recursos. La Historia Clínica Electrónica es una herramienta más para lograrlo[2].

La HCE se integra en la estrategia de la Organización Mundial de la Salud para alcanzar una cobertura sanitaria universal de acceso oportuno y equitativo. Para alcanzarlo, las tecnologías de la información y la comunicación (TIC) así como las nuevas tecnologías que suponen la incorporación de los procesos basados en la Inteligencia Artificial (IA) abren un abanico enorme de posibilidades para agilizar y hacer más eficaces la planificación en salud. A la par, desde lo jurídico nacen nuevas preguntas sobre la centralidad de la autonomía y libertad de la persona humana en los procesos de digitalización de las historias clínicas en soporte papel y la implementación de la historia clínica electrónica, a los que se aúna el rol central de la seguridad y la privacidad.

La ley 26.529 en su artículo 12 define a la historia clínica como un "documento obligatorio, cronológico, foliado y completo en el que conste toda actuación realizada al paciente por profesionales y auxiliares de salud". Este concepto se complementa en el artículo 13, que conceptualiza a la historia clínica informatizada como aquella que se confeccione en soporte magnético.

Ambas definiciones deben ser precisadas en su contenido y alcance atento el actual contexto tecnológico.

En este sentido, el artículo 8 de la ley 27.706 considera como tal al "documento digital, obligatorio, con marca temporal, individualizada y completa, en el que constan todas las actuaciones de asistencia a la salud efectuadas por profesionales y auxiliares de la salud de cada paciente, refrendadas con la firma digital del responsable".

Se incardina en la línea de otras definiciones de carácter internacional[3], en que la forma longitudinal o marca temporal permite la incorporación y registro de la información de salud que proviene de fuentes (sistemas de salud público, privado u obra social) y actores (pacientes, médicos, administrativos, informáticos, farmacéuticos) diversos. Ello supone, además, la posibilidad de una implementación interjurisdiccional para lo que se requiere asistencia técnica, financiera y de recursos humanos. A ello refiere el artículo 2, incisos c), e) y f).

En la estrategia de la Organización Mundial de la Salud, así como de la Organización Panamericana de la Salud, la interoperabilidad de los sistemas de información permitiría a dar soporte a todo el sistema asistencial, para lo cual proponen diversos estándares que son revisables en forma periódica.

Es definida como "…la capacidad de diferentes sistemas de información en salud (sistemas hospitalarios, departamentales, registros clínicos, electrónicos, etc.) para intercambiar datos y usar la información que ha sido intercambiada dentro y a través de los límites de la organización, con el fin de mejorar la prestación efectiva de los cuidados de salud a individuos y comunidades…"[4].

En esta línea, la resolución 115/2019 de la Secretaría de Salud en 2019, como parte de la estrategia para la Cobertura Universal de Salud, crea la Red Nacional de Interoperabilidad en Salud, que en su anexo define a la interoperabilidad como "habilitación de dos sistemas de información y utilizar la información compartida. Ello implica la trasferencia de información estructurada que puede descomponerse y analizarse en el sistema de destino, para ser integrada con información local y de otras fuentes"[5].

Del análisis de los artículos 1 y 3 de la ley, se desprende que la norma hace referencia a denominada "interoperabilidad organizacional" que supone una estructura multisectorial que permite comunicar y transferir las informaciones o datos. Esta estructura admite el uso de diversos sistemas de información (HCE, Historia Clínica Digital, Historia Clínica en soporte papel), una estructura e infraestructura multisectorial (público, privada, obra social), ámbitos geográficos con desarrollo muy disímil (nación, provincia, municipio)[6].

El éxito de la interoperabilidad está atado a la articulación con técnicas administrativas de coordinación y colaboración que permitan articular las diferencias que puedan existir, a la voluntad política de hacerlo y la posibilidad de garantizar la seguridad del tráfico de los datos que circulan en este sistema. Junto a ello, los modelos estandarizados de gestión y las normas de autorregulación (Códigos de Buenas Prácticas, Protocolos) pueden contribuir en este proceso.

El artículo 2 delega en la autoridad nacional de aplicación (a designar a través de reglamentación) la creación y conformación de un "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas", la determinación de las características técnicas y operativas para llevarlas adelante (esto es, estándares a implementar). El artículo 2, inciso g), le atribuye al Programa el generar un marco de interoperabilidad entre los sistemas que se encuentren en funcionamiento con los sistemas a crear, tanto en el sector público, privado y en el ámbito de la seguridad social.

Como se dijo, Argentina es un país federal en el que las competencias en materia de salud son ejercidas de manera concurrente por el Estado Nacional, por las provincias, así como por los municipios. En lo que hace a las prestaciones asistenciales de salud, conviven tres sistemas: el público, el privado y el de seguridad social.

---

entrada en vigencia de la ley y en su artículo 14 establecía la convivencia entre ambos soportes hasta la completa implementación del sistema.

(2) Luna, D. y Plazotta, F., "Historia Clínica Electrónica". Ministerio de Salud de la República Argentina, marzo de 2017. Disponible en: Historia clínica electrónica | DELS (salud.gob.ar) (fecha de consulta 10/04/2023).

(3) Healthcare Information and Managment Systems Society (HIMSS, 2018). "La HCE es un registro electrónico longitudinal de la información de salud del paciente generada por una o más interacciones en un entorno de prestación de servicios médicos. Esta información incluye datos demográficos del paciente, notas, su evolución, problemas, medicamentos, signos vitales, historial médico, inmunizaciones, datos de laboratorio y reportes de radiología". Citada en Bastías-Butler E. y Ulrich, A., "Transformación digital del sector salud en América Latina y Caribe. La Historia Clínica Electrónica. Banco Interamericano de Desarrollo, 2019. Disponible en: Transformación digital del sector salud en América Latina y el Caribe: La historia clínica electrónica | Publications (iadb.org), p. 4, (fecha de consulta: 24/03/2023).

(4) Organización Panamericana de la Salud; Organización Mundial de la Salud. *Revisión de estándares de interoperabilidad para la eSalud en Latinoamérica y el Caribe.* Washington, D.C., 2016. Disponible en: 9789275318812_spa.pdf (paho.org) (fecha de consulta 10/04/2023), pp. 14 a 18.

(5) Ministerio de Salud y Desarrollo Social. Secretaría de Gobierno de Salud. Res. 115/2019, Anexo. BO disponible en: Texto completo | Argentina.gob.ar (fecha de consulta 10/04/2023).

(6) Bastias-Butler, E.; Ulrich, A. *Transformación digital del sector salud en América Latina y el Caribe. La Historia Clínica Electrónica.* Banco Interamericano de Desarrollo, Washington, 2018. Disponible en: Transformación_digital_del_sector_salud_en_América_Latina_y_el_Caribe_la_historia_clínica_electrónica_es_es.pdf (iadb.org) (fecha de consulta 10/04/2023). Las autoras presentan un informe sobre el "Diálogo Regional de Política de la División de Protección Social y Salud". Uno de los expositores, W. Hammond, distingue nueve tipos de interoperabilidad: semántica; del consumidor; de redes y comunicaciones; funcional; de negocios; internacional; de partes interesadas; de seguridad-privacidad; legal, ética y de la sociedad (pp. 13 y 14).

Este es uno de los claroscuros de la norma. ¿Cómo articular en un Programa Federal realidades e intereses tan distintos entre jurisdicciones y sectores?, ¿cómo poner en marcha un Sistema Único de Registro de Historias Clínicas Electrónicas cuando la realidad nos muestra que el soporte papel es el único factible para poder dejar constancia de la praxis en aquellos lugares donde el acceso a Internet es nulo o dificultoso, o que en muchos casos el personal sanitario es escaso o no está capacitado?

La norma en este punto se avizora de difícil aplicación, pues delega en una autoridad de aplicación (sin plazo para su designación) la implementación de un Sistema sin plazo máximo(7), y le atribuye facultades para el establecimiento de estrategias en contextos tan dispares.

En la Unión Europea, la Comisión realizó una encuesta entre los meses de agosto y diciembre de 2020 sobre el desarrollo de HCE interoperables entre los Estados miembros, así como Noruega y el Reino Unido, a consecuencia de la adopción en 2019 de la Recomendación de la Comisión sobre el formato de intercambio de las HCE. Las preguntas versaron sobre el contexto jurídico y reglamentario; el nivel organizativo; las inversiones financieras; la seguridad y el acceso; la interoperabilidad semántica y la interoperabilidad técnica; el nivel de uso real de la HCE interoperable; el uso de HCE y macrodatos para la alerta rápida y la vigilancia, así como el diagnóstico digital del COVID-19.

Los resultados son muy disímiles entre los países, pues juegan diversas variables, a saber: su extensión territorial, su organización política (centralizado o federal) y también la capacidad para su puesta en marcha. En el informe se destaca que muchos de los pacientes no pueden acceder a sus datos o usarlos o transmitirlos a sus prestadores de salud. Países como Estonia o Finlandia llegaron a la interoperabilidad plena entre regiones; España tiene un grado de digitalización alta, pero su sistema de organización política (comunidades autónomas uni o pluriprovinciales) lleva a una gran descentralización que se plasma en una muy baja interoperabilidad. Otro grupo de países, como República Checa, Lituania, Letonia, Polonia o Eslovenia, pueden enviar o recibir resúmenes de historiales de pacientes fuera de sus fronteras(8).

Estas experiencias corroboran lo dificultoso que es poner en marcha este programa, así como la creación del Sistema Único que será quien maneje la totalidad de los datos de salud de los pacientes sin posibilidad de prestar consentimiento para ser parte o retirarse de este sistema, sin pautas de seguridad para la protección de sus datos personales o el posible uso secundario de datos.

III. Segundo claroscuro. El consentimiento informado del paciente

El Sistema de Registro Único persigue la creación de un banco de datos de información sensible como lo son los referidos a la salud de las personas que quedará en manos de una autoridad de aplicación no definida, así como también, sin pautas sobre los lineamientos a seguir sobre su tratamiento.

El dictado de la Ley de Protección del Paciente fue un gran paso para dejar de lado el paternalismo sanitario y fortalecer la autonomía del paciente que tiene una de sus máximas expresiones en el consentimiento informado, así como en la posibilidad de recibir o no tratamiento o información vinculada a él.

En este caso, el camino se recorre a la inversa. El Estado se hace con una base de datos en la que no se requiere el consentimiento informado de los pacientes o de sus representantes tanto en lo que hace al Registro como al Sistema.

El Estado se abroga la ley 26.529 y el artículo 59 del CCyC por cuanto la creación de un Sistema Único de Registro de Historias Clínicas es un registro de datos de salud en el que el dato es una expresión de la autonomía de la voluntad, pero es también contenido y continente de esa Historia Clínica.

La incorporación compulsiva de las historias clínicas a este registro cercena derechos y libertades, pues no requiere de un consentimiento, asentimiento o autorización. No permite al paciente expresar su deseo de estar en él o no; no permite solicitar el retiro del sistema; no permite a los familiares retirar los datos del sistema en el caso de fallecimiento o ausencia con presunción de fallecimiento; no permite que los terceros que puedan verse afectados puedan solicitar el retiro de datos.

Múltiples "noes" que son la muestra de un Estado intervencionista, pero ineficaz. La creación de un Sistema Único no garantiza al ciudadano un sistema de salud más eficaz, con prestaciones cubiertas, sin demoras y con calidad. Es acrecentar la burocracia estatal que encarece costos y obstaculiza una posible mejora.

Como bien lo señala el artículo 14 de la Ley de HCE el titular del documento es el paciente, no lo es el Estado ni el prestador de salud.

El consentimiento es el instrumento con el que cuenta el titular de la HCE para equilibrar la asimetría existente que debe sustentarse, además, en la confianza y en la confidencialidad de la información aportada, suministrada u obtenida.

No puede interpretarse que el consentimiento informado prestado para la praxis que se vuelca en la HCE sea un consentimiento abierto o en blando, dado que la información no se halla anonimizada o seudonimizada.

El consentimiento para incorporarse o la posibilidad de retirarse del Sistema de Registro es una doble garantía para el paciente, suprimida en esta ley, sobre la disposición de sus datos, así como la posibilidad de contralor de las actividades de la organización del sistema de salud desde la perspectiva de la seguridad sobre el manejo de datos.

Por otro lado, al ser compulsiva la integración de las HCE al Sistema de Registro, cabe la pregunta sobre la validez de las presunciones en derredor a la validez de la HCE así integrada. La presunción ¿se extiende fuera de la órbita de la entidad generadora o colaboradora en la formación del documento del paciente o, por el contrario, se extiende a la autoridad de aplicación estatal?

Si extendemos la presunción a la autoridad de aplicación y se producen quiebres, fuga de datos, hackeos o uso secundario o indebido de datos en lo que hace a la reparación de daños, ¿cuál es el régimen de prevención y reparación aplicable?

Y, en esta serie de interrogantes, cabe preguntarse sobre la posibilidad de ceder los datos del usuario (aun anonimizados) para otros fines que no se correspondan con su uso por parte del sistema de salud, que puedan generar situaciones como discriminación en forma negativa, derivar en la incorrecta utilización de datos o traspaso a terceros ajenos al ciclo vital de los datos o destinar la información a la creación de algoritmos de carácter predictivo.

IV. Tercer claroscuro. Vulnerabilidad en la protección de datos personales

En estrecha relación con la necesidad del consentimiento del titular de la HCE tanto para la conformación como para el retiro del Sistema de Registro y sobre la disposición de sus datos, se presenta otra falencia normativa en lo que hace a su protección.

En efecto, se advierte una mayor vulnerabilidad por cuanto los datos allí volcados pueden ser destinados al ámbito sanitario, a la investigación científica así como el expresado uso secundario de esta información. Este registro compulsivo no trae consigo las soluciones jurídicas suficientes de protección.

El texto de la ley recurre en varias oportunidades a los vocablos "confidencialidad" y "estricto" en alusión a la seguridad de los datos y el cumplimiento de lo establecido en ella.

Al énfasis propuesto se le opone la incerteza sobre el cómo se van a implementar estas herramientas basadas en una norma como la Ley de Protección de Datos, que debió ser actualizada y modificada en forma previa al dictado de una norma de estas características. Algo así como construir una casa por el techo y no por las bases.

La norma es un desafío para la protección de los datos personales. El almacenamiento masivo de datos sensibles (como lo son los datos de salud) en una base de datos monopolizada por el Estado puede generar nuevas vulnerabi-

(7) En el Proyecto de Ley presentado por la senadora Najul, en su artículo 6, se indicaba un plazo máximo de implementación de tres años a contar desde la entrada en vigencia de la norma. En su artículo 9 proponía que el Ministerio de Ciencia, Tecnología e Innovación fuese el responsable del diseño y administración del sistema informático de interconectividad para desarrollar una plataforma interoperable. Proyecto completo disponible en: 4172-D-2020.pdf (hcdn.gob.ar) (fecha de consulta 10/04/2023).

(8) Comisión Europea. *eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the EU*. Bruselas, 2021. Disponible en: Interoperabilidad de los historiales médicos electrónicos en la UE | Configurar el futuro digital de Europa (fecha de consulta 10/04/2023).

lidades. Las posibles violaciones de seguridad impactan en la privacidad y en la confidencialidad de tales datos.

En estos sistemas es necesaria la evaluación en forma permanente de los posibles riesgos de filtraciones, hackeos u otras actividades delictivas con miras a proveerse de millones de datos que no solo impactan en su titular, sino en terceras personas.

En el sistema de salud se mueven millones de datos personales, muchos de los cuales son brindados de manera espontánea por el paciente, en otros casos son el resultado de pruebas, exámenes o consultas, recetas digitales, recetas electrónicas, los metadatos fruto de la realización de exámenes genéticos o la mediación digital en consultas, exámenes o intervenciones, a modo de ejemplo.

A la par, estas tecnologías basadas en sistemas de Inteligencia Artificial no escapan a las consideraciones éticas sobre la forma del procesamiento de datos, los fenómenos de cajas negras o el desarrollo de las nuevas tecnologías con capacidades no mensurables para el proceso de datos como lo son los recientes Chats de OpenAI o la interoperabilidad en el marco del Internet de las Cosas.

La gobernanza de datos es un esquema complejo en el que deben ponderarse la complejidad y la utilidad del análisis, desde el momento de la apertura de la historia clínica hasta el análisis de esos datos de una manera descriptiva, predictiva y prescriptiva frente a la protección del sistema, de los profesionales y de los pacientes.

Como todo dato, los datos de salud también tienen un ciclo vital que en el caso del Programa no parece quedar claro. En este sentido, entre los claroscuros se advierte que no se indica qué sucede con los datos almacenados de una persona que fallece o deja de residir en el país, la protección de los terceros que puedan verse afectados por el tratamiento de esos datos o la conversión de dichos datos en metadatos (por ejemplo, a los fines de investigación) y, por tanto, con un ciclo vital marcado por la anonimización o la seudonimización.

Este ciclo de obtención o generación de datos, y los métodos para su almacenaje, evaluación, borrado, anonimizado, recuperación, manipulación, serán determinados entonces por la autoridad de aplicación.

La pléyade de atribuciones conferidas a la autoridad de aplicación parece más declamatoria que factible de implementar en la práctica y, sobre todo, en el marco del desarrollo de los principios de gobernanza y de transparencia en una actividad de estas características por parte del Estado Nacional.

Esta gobernanza y transparencia en materia de datos requiere de una actualización de la normativa de protección de los datos personales de manera de asegurar la existencia de fiscalización interna y externa en miras a la preservación, la transmisión, la modificación y el uso compartido de información. Una modificación legislativa centrada en la actualidad de las tecnologías que transforman el sistema de protección de datos en general y en materia de salud en particular. El abanico cada vez mayor de innovaciones tecnológicas, las nuevas formas de la relación entre médico y paciente, la genética como mecanismo de diagnóstico y tratamiento, permiten la creación de volúmenes de datos en los que confluyen la autonomía del paciente, la exposición de los terceros, la participación de diversos actores en la formación de la historia clínica electrónica en los que la protección de esos datos se erige como escudo protector de un usuario de salud cada vez más vulnerable.

Argentina incorporó la norma ISO SO 27799:2016 que proporciona pautas para los estándares de seguridad de la información organizacional y de las prácticas de gestión de esa seguridad. Ello abarca la selección, la implementación y la gestión de los controles en un marco de especial riesgo, como es el tratamiento de los datos, base del sistema. Esta norma de estandarización complementa la ISO/IEC 27002 en materia de informática de salud[9]. Ella permite a los prestadores de salud y los gestores de riesgo garantizar un nivel mínimo de seguridad apropiado para cada organización en miras a mantener la confidencialidad, la integridad y la disponibilidad de la información de salud.

La normativa se aplica a todas las formas de las que se pueden obtener datos de salud (palabras, números, grabaciones de sonido, dibujos, esquemas, videos, imágenes) provenientes de soportes diversos y sistemas de almacenaje y es un punto de partida a ser considerado por la autoridad de aplicación.

Sin embargo, quedan pendientes para la urgente y necesaria reforma de la Ley de Protección de los Datos Personales, temas centrales para la protección de los derechos de los pacientes y de los diversos actores del sistema de salud. Entre ellos se destacan:

a) Metodologías y estadísticas para los procesos de anonimización efectiva de datos y toda información personal de salud.

b) Metodologías para la identificación, desidentificación o seudonimización de la información personal de salud.

c) Calidad mínima de servicio de la red, y la determinación de métodos para la medición de las redes para el uso en informática sanitaria (capacidad para soportar el tráfico seguro de datos).

V. Compás de espera. Reglamentación

Las aspiraciones de la norma no se condicen con el desarrollo de su articulado. Claroscuros en que la confidencialidad y el estricto cumplimiento se presentan como declaraciones, necesitan ser despejados a través de la reglamentación de la norma por el Poder Ejecutivo y la urgente modificación de la Ley de Datos Personales en miras a la protección reforzada de los datos personales. En ese entonces este primer análisis podrá ser profundizado para, ojalá, poder dejar de lado las críticas aquí vertidas y aspirar a lograr un sistema de salud integrado que brinde atención y cuidado a todos los ciudadanos por igual y en cualquier lugar de la geografía argentina.

VOCES: HISTORIA CLÍNICA - PROTECCIÓN DE DATOS PERSONALES - TECNOLOGÍA - PERSONA - CONSTITUCIÓN NACIONAL - INTIMIDAD - DERECHOS Y GARANTÍAS CONSTITUCIONALES - INFORMÁTICA - INTELIGENCIA ARTIFICIAL - DERECHOS PERSONALÍSIMOS - ORDEN PÚBLICO - HÁBEAS DATA - DERECHOS HUMANOS - SECRETO PROFESIONAL - DAÑOS Y PERJUICIOS - DAÑO MORAL - DAÑO PSÍQUICO - RESPONSABILIDAD CIVIL - MÉDICO - MEDICAMENTOS - CONTRATOS - OBLIGACIONES - CÓDIGO CIVIL Y COMERCIAL - ACTOS Y HECHOS JURÍDICOS - COMERCIO E INDUSTRIA - SALUD PÚBLICA - CONSENTIMIENTO - PRUEBA - CARGA DE LA PRUEBA - POLÍTICAS PÚBLICAS - HOSPITALES Y SANATORIOS - MÉDICO - OBRAS SOCIALES - DERECHOS DEL CONSUMIDOR - MEDICINA PREPAGA - PROFESIONALES DE LA SALUD

(9) Norma IRAM ISO/IEC 27002:2008.

Derecho médico e informatización y digitalización de historias clínicas

por Roberto A. Vázquez Ferreyra(*)

Sumario: I. La evolución e inflación normativa en el derecho de la salud argentino y la nueva ley 27.706. – II. Apuntes preliminares sobre la ley 27.706. – III. Conclusiones con final abierto.

I. La evolución e inflación normativa en el derecho de la salud argentino y la nueva ley 27.706

Desde hace más de dos décadas venimos hablando de una nueva rama del derecho cual es el Derecho Médico. Se trata de una rama específica del ordenamiento jurídico que a esta altura tiene un marco normativo propio –cada vez más extenso–, abundantes estudios doctrinarios como así también jurisprudencia específica, lo que configura todo un cuerpo doctrinario y jurisprudencial, y todo ello alrededor de una materia específica en la que encontramos institutos propios como los derechos de los pacientes, el consentimiento informado, la historia clínica, el rechazo de tratamientos, donación de órganos, etc.

Desde el punto de vista normativo encontramos muchas leyes dictadas tanto por la nación como por las provincias. Muchas veces incluso se genera una superposición normativa, lo que tal vez obedece al desconocimiento de principios constitucionales. Es que lo referido a la salud y medicina en general no es materia que las provincias hayan delegado a la nación. Así es como, por ejemplo, tenemos una ley nacional de sangre (ley 22.990) y en Santa Fe una ley provincial de sangre (ley provincial 10.725). Lamentablemente esta situación muchas veces es ignorada hasta por los propios operadores, tanto del sector jurídico como de salud. En cierta ocasión nos tocó intervenir en un juicio tramitado en la provincia de Santa Fe en donde estaban en juego cuestiones referidas a transfusiones de sangre y contagio de enfermedades. Al leer la sentencia de primera instancia nos sorprendió ver que estaba fundada totalmente en la ley nacional de sangre y ni mencionaba la ley provincial que era la realmente aplicable. El tema se concilió en segunda instancia, pero no teníamos dudas que podíamos estar frente a una sentencia de primera instancia nula. De hecho, así como existe una ley nacional de ejercicio de la medicina, muchas provincias, como Santa Fe, tienen su propia ley reguladora.

El Código Civil y Comercial contiene artículos directamente aplicables en el campo de la salud y tratamientos médicos. Así por ejemplo arts. 17; 55; 56; 57; 58; 59; 60; etc.

Desde la jurisprudencia encontramos pronunciamientos de tribunales internacionales. Así por ejemplo la sentencia del 16 de noviembre de 2022 de la Corte Interamericana de Derechos Humanos (Corte IDH) en el caso "Brítez Arce y otros vs. Argentina"[1], causa en la cual nuestro país se allanó a la pretensión de los reclamantes, lo que no deja de generar cierta perplejidad porque desde nuestra humilde opinión, el caso tal vez hubiera merecido una mayor defensa por parte del Estado. La cuestión excede la naturaleza de este comentario, pero se trata de un caso internacional que merece más atención por cómo se defendió nuestro país.

La inflación normativa en materia de salud es notoria, y nos preguntamos si los profesionales de la salud están o pueden estar al tanto de todo ese material; más allá de que la ley se supone conocida por todos, lo cual sabemos es una mera ficción. Ni que hablar de la doctrina y jurisprudencia. No olvidemos por ejemplo que algo tan importante como el consentimiento informado llegó a nuestro país a través de la doctrina y jurisprudencia, y recién después de muchos años tuvo regulación legal[2]. Esto nos ha llevado a pensar que los estudiantes de medicina deberían cursar paralelamente la carrera de abogacía, o al menos algún curso de formación en Derecho médico que actualmente excede el marco de la clásica materia de "medicina legal".

Menor preocupación nos genera la situación de los responsables de instituciones sanitarias, obras sociales, financiadoras, prepagas, etc., pues cuentan –o deberían contar– con otros medios, y pueden tener un asesoramiento acorde con la importancia de cada una de ellas. Lo que resulta inconcebible es que a esta altura no cuenten con comités específicos, ya sean de bioética, de prevención de riesgos, o como se los quiera llamar y que tengan por finalidad el análisis e implementación de todas las novedades que se van produciendo, paralelamente a la prevención de riesgos en la atención de pacientes.

A mero título de ejemplo, recuerdo haber dado una charla frente a un auditorio integrado por profesionales y empresarios de la salud y comprobar que muchos desconocían la entrada en vigencia de la ley 26.529 de "Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud", que había venido a generar profundos cambios en el ejercicio de la medicina. Así por ejemplo todo lo referido al consentimiento informado fue objeto de un cambio profundo a partir de la sanción de la ley citada, con lo que mucho que se escribió con anterioridad quedó profundamente desactualizado. Lo mismo puede decirse de la Historia Clínica, a la que en algún momento mencionamos como el ABC del acto médico.

Todo esto nos genera cierta preocupación, cual es la de que los médicos a la hora de tratar a un paciente estén pensando más en las normas jurídicas aplicables, que en la propia *lex artis,* que debería ser la que indique lo que puede resultar más beneficioso para el paciente, más allá del pleno y absoluto respeto por su autonomía. Ni hablar del tema de la medicina a la defensiva que ha sido tratado desde hace décadas en Estados Unidos, lo que implica un encarecimiento de la salud.

En esta oportunidad, nos convoca la ley 27.706 que lleva el ampuloso nombre de "Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina", publicada en el Boletín Oficial del 16 de marzo de 2023.

II. Apuntes preliminares sobre la ley 27.706

Lo más rescatable del nombre de la ley 27.706 es el uso de la palabra "Programa", pues la ley por ahora no es más que eso, un programa en el sentido que lo define la RAE: "previa declaración de lo que se piensa hacer en alguna materia u ocasión"[3].

Estamos convencidos de que no toda ley que dicte el Congreso debe necesariamente ser reglamentada, pero no

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *La indemnización correspondiente por la no obtención del consentimiento informado en la praxis médica,* por Roberto A. Vázquez Ferreyra, ED, 197-709; *Historia clínica. Encuadre probatorio. Responsabilidad médica. Responsabilidad omisiva,* por Lucía Graciela Savarese, ED, 216-642; *El derecho a la salud como derecho social. Garantía de la dignidad del hombre,* por Violeta Castelli, EDA, 2007-743; *El plazo de la prescripción liberatoria en materia de responsabilidad médica en los hospitales de la Ciudad Autónoma de Buenos Aires,* por Inés Amura, Esteban Centanaro y Juan Pablo Rodríguez, ED, 234-708; *Responsabilidad médica por mala praxis,* por Mariano Gagliardo, ED, 251-465; *Los médicos y el consentimiento informado (Necesarias precisiones sobre el tema en el marco del nuevo CCC),* por Marcelo J. López Mesa, ED, 266-703; *La doctrina de la "real malicia" y el derecho a la información sobre cuestiones médicas,* por María Angélica Gelli, ED, 277; *Consentimiento informado de las personas con discapacidad en tratamientos médicos,* por Nicolás Pildayn y Marina M. Sorgi Rosenthal, ED, 279; *La protección de los datos personales en internet (una tarea ineludible),* por Esteban Ruiz Martínez, ED, 284-726; *Datos personales: Google se asocia con el sistema de salud más importante de Estados Unidos,* por Laura Belén Yachelini, ED, 286-618; *El médico y la virtud de la prudencia en tiempos de pandemia,* por Germán Calabrese, ED, 289-1581; *Odontólogos. Responsabilidad civil profesional en tiempos de pandemia,* por Dante Gómez Haiss, 289-1434; *La responsabilidad del médico especialista,* por Milton H. Kees, ED, 290; *La regulación del derecho a la imagen y el régimen de protección de datos de carácter personal. Ciertas "fricciones" entre ambos regímenes,* por Guillermo F. Peyrano, ED, 290-637; *Responsabilidad del médico: necesidad de deslindar el casus de la no culpa,* por Federico Ossola y Julieta Bollero Hauser, ED, 291; *El derecho a la información de salud y el hábeas data específico,* por Eduardo Molina Quiroga, ED, 294; *Derecho a la intimidad de los datos de salud,* por Julián Prieto, ED, 300. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Doctor en Derecho y Ciencias sociales (UBA). Premio Facultad (UBA). Ex Juez de Primera Instancia Civil y Comercial de Rosario. Profesor de derecho de daños y de las obligaciones.

(1) Corte IDH, Caso *Brítez Arce y otros vs. Argentina,* sentencia de 16 de noviembre de 2022 (Fondo, Reparaciones y Costas).

(2) Veánse, entre otros, Pelle, W. D., *Los Derechos del paciente,* EUDEM, Mar del Plata, 2021; Gil Domínguez, A. (dir). *Muerte Digna,* La Ley, 2013; Weingarten, C. y Lovece, G. (dir), *Tratado de Derecho a la Salud,* La Ley, 2ª edición actualizada, 2020.

(3) RAE, Diccionario de la lengua española (actualización 2022), consulta de la voz: "Programa", segunda acepción: https://dle.rae.es/programa (fecha de consulta 8/5/2023).

nos cabe duda de que la ley 27.706 en tanto no sea reglamentada, no será más que un listado de propósitos del legislador[4]. La propia ley, en su art. 2º, delega en el Poder Ejecutivo lo que consideramos son las tareas fundamentales que surgen del nuevo marco normativo[5].

En cuanto al federalismo, quedaría resguardado por lo dispuesto en el art. 2º inc. a) que ordena al Poder Ejecutivo crear y conformar con las provincias y CABA la estructura organizativa correspondiente.

Como iniciativa nos parece un gran paso en beneficio de los pacientes. Pero somos conscientes también de los riesgos que implica en una sociedad en la que el *ciber* crimen está a la orden del día y en la cual los *ciber* delincuentes se manejan con absoluta impunidad, al menos por ahora en lo que refiere a estafas bancarias. Pero no es menos cierto que toda la intimidad referida a la salud de cada uno de los habitantes puede quedar más expuesta de lo normal, sobre todo si no se encara la cuestión con la seguridad que ello exige.

El legislador ha advertido dicha peligrosidad al hacer expresa referencia a la ley de Derechos del Paciente (26529) y ley de Protección de los Datos Personales (25.326). En este punto, la clave pasa por el art. 7, inc. b) según el cual "el sistema informático deberá impedir que los datos sean leídos, copiados o retirados por personas no autorizadas". Esta disposición debería ser acompañada por una norma penal específica que con altas penas castigue a quienes infrinjan lo dispuesto, lo que exige una correcta tipificación.

Hace muchos años, en los inicios de internet, pensábamos en lo beneficioso que podía ser que la historia vinculada a la salud de una persona (desde antes de su nacimiento y "hasta su fallecimiento"; art. 4 de la ley 27.706[6]) se encuentre registrada en un documento único que pudiera ser consultado por cualquier profesional que atienda a esa paciente, con las debidas autorizaciones. Ello permitiría conocer todo el historial médico, antecedentes y demás información necesaria para la atención médica. Pero claro, en aquellos momentos no estaban aún encendidas las alarmas por la delincuencia informática. Y eso creo que debe ser una de las mayores preocupaciones en la implementación progresiva de la nueva ley.

Por ello, resulta fundamental el determinar la forma de ingreso, estableciendo diversos niveles de acceso a la información (no es lo mismo el médico de cabecera que el enfermero de piso en una internación), como así también las medidas de protección para evitar ingresos o adulteraciones ilegales. A eso hace referencia el art. 7, inc. a), que habla de un mínimo de tres niveles de acceso[7]. Esto es fundamental sobre todo en una sociedad como la nuestra en que los *ciber* criminales se manejan impunemente.

Observamos que el legislador manda crear una Comisión Interdisciplinaria de expertos garantizando la representación proporcional de los subsistemas. Por nuestra parte, pensamos que sería muy útil que la reglamentación cree también una comisión o subcomisión integrada por expertos en derecho médico y bioética para que pueda actuar como órgano de consulta frente a casos que puedan ser problemáticos y exijan la opinión de expertos.

La ley no establece un plazo durante el cual se deberá guardar la información, pero estimamos que sería prudente establecer hasta 5 años de conocido el fallecimiento del paciente en cuestión.

Llama la atención el inc. f), del art. 2, en cuanto dispone que el Sistema Único de Registro de Historias Clínicas Electrónicas "debe ser auditable y pasible de ser inspeccionado por las autoridades correspondientes". Tal disposición siembra una cuota de temor. ¿Qué es lo que van a auditar o inspeccionar? ¿A qué información tendrán acceso? ¿El acceso será sin afectar la privacidad de la información? Son muchas las inquietudes que nos genera el hecho de que alguna dependencia pública pueda tener acceso a toda la información referida a aspectos privados de la salud de cada uno.

El art. 2º, inc. g), terminaría con la necesidad del secuestro de historias clínicas pues, por ejemplo, en un proceso de responsabilidad civil médica le bastaría al paciente bajar la información o bien tener acceso a ella junto a su consultor técnico. En concordancia, el art. 8º, dispone que el paciente es titular de los datos y tiene en todo momento derecho a conocer la información en la historia clínica.

En su parte final, el art. 8º (párrafo tercero), aclara todo lo que debe estar contenido en la historia clínica electrónica (indicaciones médicas, consentimientos informados, planillas de enfermería, prescripciones dietarias, etc.). Obvio que se trata de una mención meramente enunciativa.

Finalmente, la ley dispone que "en caso de incapacidad del paciente o imposibilidad de comprender la información a causa de su estado físico o psíquico, la misma debe ser brindada a su representante legal o derecho habientes, conforme lo establecido en la ley de protección de datos personales y sus modificatorias" (art. 8, párrafo cuarto).

Nos queda un interrogante. Es de suponer que para ingresar a la historia clínica informatizada será necesario contar con un PIN o Token del que sólo tendrá conocimiento y acceso el propio paciente o sus representantes. Supongamos que un paciente plenamente capaz que sufre un accidente y requiere ser atendido mientras se encuentra privado de la razón. En tal caso, nos queda el interrogante de cómo se podrá acceder a la HCI, pues suponemos que la información de acceso solo la tendrá el paciente, quien a su vez la podrá cambiar tantas veces como desee y cuando lo desee. Tal vez esto sea contemplado por la reglamentación.

III. Conclusiones con final abierto

En definitiva, aplaudimos esta ley en cuanto puede implicar un gran avance en el cuidado de la salud, pero nos quedan todos los temores que genera el hecho de que terceros puedan tener acceso a datos que hacen a la mayor intimidad del ser humano. La reglamentación deberá ser muy cuidadosa y estar en manos de los mejores expertos.

VOCES: HISTORIA CLÍNICA - PROTECCIÓN DE DATOS PERSONALES - TECNOLOGÍA - PERSONA - CONSTITUCIÓN NACIONAL - INTIMIDAD - DERECHOS Y GARANTÍAS CONSTITUCIONALES - INFORMÁTICA - INTELIGENCIA ARTIFICIAL - DERECHOS PERSONALÍSIMOS - ORDEN PÚBLICO - HÁBEAS DATA - DERECHOS HUMANOS - SECRETO PROFESIONAL - DAÑOS Y PERJUICIOS - DAÑO MORAL - DAÑO PSÍQUICO - RESPONSABILIDAD CIVIL - MÉDICO - MEDICAMENTOS - CONTRATOS - OBLIGACIONES - CÓDIGO CIVIL Y COMERCIAL - ACTOS Y HECHOS JURÍDICOS - COMERCIO E INDUSTRIA - POLÍTICAS PÚBLICAS - SALUD PÚBLICA - CONSENTIMIENTO - PRUEBA - CARGA DE LA PRUEBA - HOSPITALES Y SANATORIOS - MÉDICO - OBRAS SOCIALES - DERECHOS DEL CONSUMIDOR - MEDICINA PREPAGA - PROFESIONALES DE LA SALUD

(4) Por su parte, el art. 10, establece que "[e]l Poder Ejecutivo reglamentará la presente ley dentro de los noventa (90) días de su publicación".

(5) Art. 2°: "El Poder Ejecutivo debe determinar la autoridad nacional de aplicación de la presente, la que tiene, entre otras, las siguientes atribuciones: a) Crear y conformar con las provincias y la Ciudad Autónoma de Buenos Aires la estructura organizativa del Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina y reglamentar su implementación y su progresivo funcionamiento; b) Determinar las características técnicas y operativas de la informatización y digitalización de las historias clínicas del sistema de salud de la República Argentina; c) Elaborar un protocolo de carga de historias clínicas, así como diseñar e implementar un software de historia clínica coordinando la implementación interjurisdiccional, ajustándose a lo dispuesto por la presente y por las leyes 26.529 y 25.326 y sus normas modificatorias y reglamentarias; d) Generar un marco de interoperabilidad entre los sistemas que se encuentren en funcionamiento con los sistemas a crear, tanto en el sector público, privado y del ámbito de la seguridad social; e) Instalar el software de forma gratuita en todos los hospitales públicos, nacionales, provinciales y municipales; y, en la forma que se establezca por vía reglamentaria, en los centros de salud privados y de la seguridad social; f) Proveer asistencia técnica y financiera a las jurisdicciones provinciales y de la Ciudad Autónoma de Buenos Aires, para cumplir los objetivos de la presente ley; g) Coordinar los recursos destinados al cumplimiento de los objetivos de la presente ley; h) Crear una Comisión Interdisciplinaria de expertos garantizando la representación proporcional de los subsistemas involucrados, a los efectos de coordinar con las autoridades provinciales y de la Ciudad Autónoma de Buenos Aires, en el marco del Consejo Federal de Salud (COFESA), la implementación de la presente ley en cada una de las jurisdicciones; i) Capacitar al personal sanitario".

(6) Art. 4: "El Sistema Único de Registro de Historias Clínicas Electrónicas debe contener los datos clínicos de la persona o paciente, de forma clara y de fácil entendimiento, desde el nacimiento hasta su fallecimiento. La información suministrada no puede ser alterada, sin que quede registrada la modificación pertinente, aun en el caso de que tuviera por objeto subsanar un error acorde a lo establecido en la ley 25.326 de Protección de Datos Personales y sus modificatorias".

(7) Art. 7°: "A los efectos de la presente ley, entiéndase: a) Acceso/Accesibilidad: posibilidad de ingresar a la información contenida en las Historias Clínicas Electrónicas. Debe garantizarse que la información esté disponible en todo momento y en todos los establecimientos asistenciales. El acceso debe estar limitado tanto por el derecho fundamental a la privacidad del paciente como por los mecanismos de seguridad necesarios, entre los que se encuentra la autenticación. Existen por lo menos tres (3) niveles de acceso: el de consulta, el de consulta y actualización y por último el de consulta, actualización y modificación de la información, de conformidad con lo establecido en la presente ley [...]".

Ley 27.706

Programa Federal Único de Informatización y Digitalización de Historias Clínicas de la República Argentina

Creación.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

Capítulo I
Programa Federal Único de Informatización y Digitalización de Historias Clínicas de la República Argentina

Artículo 1° – Créase el Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina con la finalidad de instaurar, en forma progresiva, el Sistema Único de Registro de Historias Clínicas Electrónicas, respetando lo establecido por el Capítulo IV de la ley 26.529 de Derechos del Paciente en su relación con los Profesionales e Instituciones de la Salud y por la ley 25.326 de Protección de los Datos Personales y sus modificatorias.

Artículo 2°– El Poder Ejecutivo debe determinar la autoridad nacional de aplicación de la presente, la que tiene, entre otras, las siguientes atribuciones:

a) Crear y conformar con las provincias y la Ciudad Autónoma de Buenos Aires la estructura organizativa del Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina y reglamentar su implementación y su progresivo funcionamiento;

b) Determinar las características técnicas y operativas de la informatización y digitalización de las historias clínicas del sistema de salud de la República Argentina;

c) Elaborar un protocolo de carga de historias clínicas, así como diseñar e implementar un software de historia clínica coordinando la implementación interjurisdiccional, ajustándose a lo dispuesto por la presente y por las leyes 26.529 y 25.326 y sus normas modificatorias y reglamentarias;

d) Generar un marco de interoperabilidad entre los sistemas que se encuentren en funcionamiento con los sistemas a crear, tanto en el sector público, privado y del ámbito de la seguridad social;

e) Instalar el software de forma gratuita en todos los hospitales públicos, nacionales, provinciales y municipales; y, en la forma que se establezca por vía reglamentaria, en los centros de salud privados y de la seguridad social;

f) Proveer asistencia técnica y financiera a las jurisdicciones provinciales y de la Ciudad Autónoma de Buenos Aires, para cumplir los objetivos de la presente ley;

g) Coordinar los recursos destinados al cumplimiento de los objetivos de la presente ley;

h) Crear una Comisión Interdisciplinaria de expertos garantizando la representación proporcional de los subsistemas involucrados, a los efectos de coordinar con las autoridades provinciales y de la Ciudad Autónoma de Buenos Aires, en el marco del Consejo Federal de Salud (COFESA), la implementación de la presente ley en cada una de las jurisdicciones;

i) Capacitar al personal sanitario.

Capítulo II
Sistema Único de Registro de Historias Clínicas Electrónicas

Artículo 3°- En el Sistema Único de Registro de Historias Clínicas Electrónicas se deja constancia de toda intervención médico-sanitaria a cargo de profesionales y auxiliares de la salud, que se brinde en el territorio nacional, ya sea en establecimientos públicos del sistema de salud de jurisdicción nacional, provincial o municipal, y de la Ciudad Autónoma de Buenos Aires, como en establecimientos privados y de la seguridad social.

Artículo 4°- El Sistema Único de Registro de Historias Clínicas Electrónicas debe contener los datos clínicos de la persona o paciente, de forma clara y de fácil entendimiento, desde el nacimiento hasta su fallecimiento.

La información suministrada no puede ser alterada, sin que quede registrada la modificación pertinente, aun en el caso de que tuviera por objeto subsanar un error acorde a lo establecido en la ley 25.326 de Protección de Datos Personales y sus modificatorias.

Artículo 5°- El Sistema Único de Registro de Historias Clínicas Electrónicas garantiza a los pacientes y a los profesionales de la salud, el acceso a una base de datos de información clínica relevante para atención sanitaria de cada paciente desde cualquier lugar del territorio nacional, asegurando a este que la consulta de sus datos quedará restringida a quien esté autorizado.

Artículo 6°- El Sistema Único de Registro de Historias Clínicas Electrónicas, debe cumplir con las siguientes características:

a) La información clínica contenida en el Sistema Único de Registro de Historias Clínicas Electrónicas debe tener, bajo la responsabilidad administrativa, civil o penal, carácter confidencial. La autoridad de aplicación establece los responsables de la administración y el resguardo de la información clínica;

b) La información clínica contenida en el Sistema Único de Registro de Historias Clínicas Electrónicas, su registro, actualización o modificación y consulta se efectúan en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad, acceso y trazabilidad;

c) Se deben garantizar los mecanismos informáticos para la autenticación de las personas, agentes, profesionales y auxiliares de la salud que intervengan en el Sistema Único de Registro de Historias Clínicas Electrónicas;

d) Se debe garantizar el libre acceso y seguimiento por parte del paciente;

e) El Sistema Único de Registro de Historias Clínicas Electrónicas debe contemplar la recuperación de archivos y la perdurabilidad de la información;

f) El Sistema Único de Registro de Historias Clínicas Electrónicas debe ser auditable y pasible de ser inspeccionado por las autoridades correspondientes;

g) La información contenida en el Sistema Único de Registro de Historias Clínicas Electrónicas constituye documentación auténtica y, como tal, es válida y admisible como medio probatorio, haciendo plena fe a todos los efectos, siempre que se encuentre autenticada.

Artículo 7°- A los efectos de la presente ley, entiéndase:

a) Acceso/Accesibilidad: posibilidad de ingresar a la información contenida en las Historias Clínicas Electrónicas. Debe garantizarse que la información esté disponible en todo momento y en todos los establecimientos asistenciales. El acceso debe estar limitado tanto por el derecho fundamental a la privacidad del paciente como por los mecanismos de seguridad necesarios, entre los que se encuentra la autenticación. Existen por lo menos tres (3) niveles de acceso: el de consulta, el de consulta y actualización y por último el de consulta, actualización y modificación de la información, de conformidad con lo establecido en la presente ley;

b) Confidencialidad: el sistema informático deberá impedir que los datos sean leídos, copiados o retirados por personas no autorizadas;

c) Integridad: cualidad que indica que la información contenida en el sistema informático para la prestación de servicios digitales permanece completa e inalterada y, en su caso, que solo ha sido modificada por la persona autorizada al efecto, de conformidad con lo dispuesto en la presente ley;

d) Seguridad: preservación de la confidencialidad, integridad y disponibilidad de la información, además de otras propiedades, como autenticidad, responsabilidad, no repudio y fiabilidad;

e) Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información y/o sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad, dejando rastro del respectivo acceso.

Capítulo III
Historia Clínica Electrónica

Artículo 8°- El paciente es titular de los datos y tiene en todo momento derecho a conocer la información en la Historia Clínica Electrónica que es el documento digital, obligatorio, con marca temporal, individualizada y completa, en el que constan todas las actuaciones de asistencia a la salud efectuadas por profesionales y auxiliares de la salud a cada paciente, refrendadas con la firma digital del responsable.

El almacenamiento, actualización y uso se efectúa en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad y acceso, de conformidad con la normativa aprobada por la autoridad de aplicación de la presente ley, como órgano rector competente.

Forman parte los consentimientos informados, las hojas de indicaciones médicas y/o profesionales, las planillas de enfermería, los protocolos quirúrgicos, las prescripciones dietarias, certificados de vacunación, los estudios y prácticas realizadas, rechazadas o abandonadas.

En caso de incapacidad del paciente o imposibilidad de comprender la información a causa de su estado físico o psíquico, la misma debe ser brindada a su representante legal o derecho habientes, conforme lo establecido por la ley 25.326 de protección de los datos personales y sus modificatorias.

Artículo 9°- El gasto que demande el cumplimiento del Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de la República Argentina creado por la presente ley se financiará con los créditos correspondientes a la partida que anualmente se sancione en el Presupuesto General de la Administración Pública con destino al Ministerio de Salud.

Artículo 10.- El Poder Ejecutivo reglamentará la presente ley dentro de los noventa (90) días de su publicación.

Artículo 11.- Comuníquese al Poder Ejecutivo nacional.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS 28 DÍAS DEL MES DE FEBRERO DE 2023.

REGISTRADO BAJO EL N° 27706

CLAUDIA LEDESMA ABDALA DE ZAMORA - CECILIA MOREAU - Marcelo Jorge Fuentes - Eduardo Cergnul.

VOCES: HISTORIA CLÍNICA - PROTECCIÓN DE DATOS PERSONALES - TECNOLOGÍA - PERSONA - CONSTITUCIÓN NACIONAL - INTIMIDAD - DERECHOS Y GARANTÍAS CONSTITUCIONALES - INFORMÁTICA - INTELIGENCIA ARTIFICIAL - DERECHOS PERSONALÍSIMOS - ORDEN PÚBLICO - HÁBEAS DATA - DERECHOS HUMANOS - SECRETO PROFESIONAL - DAÑOS Y PERJUICIOS - DAÑO MORAL - DAÑO PSÍQUICO - RESPONSABILIDAD CIVIL - MÉDICO - MEDICAMENTOS - CONTRATOS - OBLIGACIONES - CÓDIGO CIVIL Y COMERCIAL - ACTOS Y HECHOS JURÍDICOS - COMERCIO E INDUSTRIA - SALUD PÚBLICA - CONSENTIMIENTO - PRUEBA - CARGA DE LA PRUEBA - POLÍTICAS PÚBLICAS - HOSPITALES Y SANATORIOS - MÉDICO - OBRAS SOCIALES - DERECHOS DEL CONSUMIDOR - MEDICINA PREPAGA - PROFESIONALES DE LA SALUD