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