HCE, los derechos de los pacientes y sus aristas técnicas problemáticas. La protección técnica de datos, el tratamiento informatizado de datos de salud y la plataforma de comunicación

Johanna Caterina Faliero[1]

[1] Doctoranda, Especialista, Consultora, Abg.[da] Dip. Hon., Inv. y Profa. en Derecho Informático y Privacidad de Datos (Facd de Der. UBA). Inv. Tesista Proy. UBACyT. Inv. Adsc. Inst. Gioja. Inv. CELE (UP). Inv. PII (UBA). Inv. Inst.Der.Inf. (CPACF).

Email: dra.jcfaliero@gmail.com

Resumen. El presente trabajo versa sobre las aristas más problemáticas en la implementación de sistemas de HCE en el seno de las instituciones sanitarias. Señala la insuficiencia regulatoria de tipo práctico que presenta el régimen actual de privacidad de datos, a causa de la falta de tutela activa, dinámica y preventiva respecto de los datos de salud en todas aquellas tareas rutinarias que se efectúan en su tratamiento informatizado durante todo su ciclo de vida. Se puntualiza el alejamiento terminológico existente entre el sistema normativo y la práctica técnica-empresarial y se procede a proponer la implementación de prácticas técnicamente actualizadas y eficaces de seguridad de datos con teleología preventiva. En lo que respecta al tratamiento informatizado de datos de salud, se señalan en líneas generales sus puntos más conflictivos, y se sugiere en particular la utilización generalizada jurídica y técnica de dispositivos e-token para el paciente como todos los integrantes del personal sanitario y relacionado, en el procesamiento de las HCE. Finalmente, se analizan los caracteres de integridad y unicidad que deben poseer las HCE, marcando la relevancia fundamental de interoperabilidad del sistema y la caracterización de su arquitectura.

Palabras Clave. HCE) – Datos de Salud – Datos Personales – Protección de Datos – Privacidad – Confidencialidad – Autodeterminación Informativa – Derechos del paciente

1 Introducción

Es sabido ya, que en materia de actividad médica, la historia clínica es uno de los documentos médicos legales principales más relevantes en materia sanitaria, tanto para el paciente como para el médico. Ya sea como instrumento probatorio, herra-

mienta de trabajo y medio de conocimiento para el ejercicio de derechos fundamentales del paciente, la historia clínica se erige como un elemento conflictivo en lo que respecta el tratamiento informatizado de datos y la protección que merecen estos últimos.

En el frondoso campo de las intersecciones entre el derecho y las aplicaciones prácticas de la informática, el tratamiento informatizado de datos – *entendido como las operaciones y procedimientos sistemáticos efectuados sobre estos últimos con el objeto de su recolección, conservación, ordenamiento, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, procesamiento, comunicación, consulta, transferencia, cesión, destrucción, etc*.- se presenta como una actividad riesgosa, máxime cuando se trata del procesamiento de datos de salud, aquellos que por excelencia contiene la historia clínica.

La Ley de Protección de los Datos Personales vigente enuncia 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 éstos 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.*", al mismo tiempo que focaliza su eje protectorio en el derecho humano fundamental que posee el titular del dato que se asienta en el "banco de datos" informatizado, derecho de origen constitucional implícito, a saber, el de autodeterminación informativa.

Dentro de las clasificaciones que efectúa la norma, ingresan dentro de la categoría de "datos sensibles", los datos de salud. La Ley define a los "datos personales" como la "*Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*.", y a los "datos sensibles" como los "*Datos personales 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*."

En lo referente a la seguridad de los datos, la Ley establece 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" y la prohibición de "registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad." (Art. 9 – Ley 25326). En cumplimiento de dicha función la Disposición 11/2006 aprueba las "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados", y a tales fines establece la obligatoriedad para los "responsables registrados" un "Documento de Seguridad de Datos Personales" como "instrumento para la especificación de la normativa de seguridad, el que deberá adecuarse en todo momento a las disposiciones vigentes en la materia dictadas por la Dirección Nacional de Protección de Datos Per-

sonales" y"Tres (3) Niveles de Seguridad: Básico, Medio Y Critico, conforme la naturaleza de la información tratada …" (Disposición 11/2006 Considerando). Las medidas de seguridad de nivel crítico son de aplicación a las bases de datos que contienen datos personales definidos como datos sensibles, es decir, que toda base de datos de historias clínicas debiera ajustarse a los más altos estándares de seguridad.

Efectuado este breve racconto introductorio, se puede concluir a simple vista que jurídicamente el sistema normativo citado en particular no puntualiza una desconfianza natural formada sobre la protección de datos. Es decir, las normas referidas resguardan el dato, el derecho de su titular, y la seguridad en su tratamiento a estos fines, pero no tutelan activa, dinámica y preventivamente los datos en todas aquellas tareas rutinarias que se efectúan dentro de la actividad lícita y reglamentaria misma que implica su tratamiento informatizado en todo el ciclo de vida del mismo, aun cuando este tratamiento se ajuste a los máximos estándares de seguridad establecidos normativamente (nivel crítico), lo cual sucede a diario en con el tratamiento informatizado de datos de salud contenido en historias clínicas informatizadas/electrónicas y digitales.

2 Historia Clínica Electrónica y Derechos Involucrados

"*En la persona humana, dotada de inteligencia y libertad, reside la dignidad. Ser persona es un rango, una categoría que no tienen los seres irracionales. Esta prestancia o superioridad del ser humano sobre los que carecen de razón es lo que se llama la dignidad de la persona humana. El concepto de dignidad humana está en el centro mismo del Derecho Internacional de DDHH. Es un derecho reconocido implícitamente (Art. 33) y expresamente (Art. 75 Inc. 22) por nuestra Carta Magna. ... Hay derechos normados en la ley 26529 que tienen sustento directo en el principio dignidad. Por caso, los derechos al "trato digno y respetuoso", a la "intimidad", a la "confidencialidad", a la "muerte digna*""[1]

Ley de Derechos del Paciente[2] enumera y describe en su Art. 2 los derechos esenciales en la relación entre paciente y los profesionales de la salud, dentro de los cuales encontramos el derecho al trato digno y respetuoso, a la intimidad y a la confidencialidad, los que describe del siguiente modo: "*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: ... b) Trato digno y respetuoso. El paciente tiene el derecho a que los agentes del sistema de salud intervinientes, le otorguen un trato digno, con respeto a sus convicciones personales y morales, principalmente las relacionadas con sus condiciones socioculturales, de género, de pudor y a su intimidad, cualquiera sea el padecimiento que presente, y se haga extensivo a los familiares o acompañantes; c) Intimidad. 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 Nº 25.326;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;...." (Art. 2 Ley 26529).

Los pacientes tienen derecho a un trato digno y respetuoso respecto de sus condiciones de pudor o intimidad, a mismo tiempo que toda actividad que se deba realizar con ellos preserve un debido resguardo de la intimidad de los mismos como de la confidencialidad de sus datos sensibles. Por último, la ley enuncia el deber de reserva que debe mantener todo profesional de salud de la documentación clínica de la que tenga conocimiento por cualquier medio (elaboración, consulta, redacción, manipulación, etc.).

A su vez, el Código de Ética de la Asociación Médica Argentina también se ocupa en regular el deber de reserva, intimidad, privacidad y confidencialidad en sus Art. 182, 183, 184, 251; y por último, establece una precisión relativa a la privacidad y confidencialidad del correo electrónico en su Art. 250.

Como bien resume la doctrina local en la siguiente cita: "*Lo confidencial es "lo que se hace o se dice en confianza o seguridad recíproca entre dos o más personas" (Dicc. de la Real Academia Española). ... la persona que necesita del auxilio médico (el paciente), se brinda en confianza a la persona que posee el saber médico (el médico). De ese encuentro (intimidad-privacidad-confianza/ciencia médica), queda la información sobre los aspectos médicos y personales del paciente en la esfera de conocimiento del médico. Lo que genera el derecho del paciente y la obligación del médico al secreto médico. Por otra parte, hay información médica perteneciente al paciente (brota de su estado de salud-enfermedad) que se vuelca en la documentación clínica (soporte papel o digital), respecto de la cual: i) el paciente tiene derecho a que se guarde estricta reserva (que no se la revele; que no se la haga pública); y, ii) los integrantes del Equipo de Salud (profesional, técnico, auxiliar, administrativo), están obligados a mantener reserva sobre la información de marras. El principio de reserva puede ser excepcionado cuando es el mismo paciente quien autoriza la revelación, o también, cuando la autoridad judicial dispone expresamente la divulgación por motivos fundados. Queda claro que…los pacientes tienen derecho a la confidencialidad de sus datos médicos personales. En correspondencia con este derecho el agente sanitario debe indefectiblemente guardar y preservar el secreto profesional*."[3]

En lo específico, la privacidad y seguridad de los datos son unas de las cuestiones más importantes a considerar para cualquier registro de datos en formato electrónico, más aún si hablamos de sistemas de HCE donde los datos que se almacenan y registran poseen la más alta sensibilidad (datos de salud). La información de salud debe verse protegida y debe restringirse la capacidad de cualquier institución o sujeto de divulgar información perteneciente al paciente, a acceder a ella sin autorización suficiente.

Nuestra Ley de Derechos del Paciente en su Art. 19 establece que se encuentran legitimados para solicitar la historia clínica[4]:*" a) El paciente y su representante legal; b) El cónyuge o la persona que conviva con el paciente en unión de hecho, sea o no de distinto sexo según acreditación que determine la reglamentación y los herederos forzosos, en su caso, con la autorización del paciente, salvo que éste se encuentre imposibilitado de darla; c) Los médicos, y otros profesionales del arte de curar, cuando cuenten con expresa autorización del paciente o de su representante legal. - A dichos fines, el depositario deberá disponer de un ejemplar del expediente médico con carácter de copia de resguardo, revistiendo dicha copia todas las formalidades y garantías que las debidas al original. ..."* (Art. 19 Ley 26529).

La reglamentación de este artículo, profundiza diciendo: *"Mientras la Historia Clínica se encuentre en poder del prestador de salud que la emitió, ante la solicitud del legitimado para pedir una copia, se deberá entregar un ejemplar de la misma en forma impresa y firmada por el responsable autorizado a tales efectos. Los costos que el cumplimiento del presente genere serán a cargo del solicitante cuando correspondiere. En caso de no poder afrontar el solicitante el costo de la copia de la historia clínica, la misma se entregará en forma gratuita.- ... Cuando el original de la historia clínica sea requerida judicialmente, deberá permanecer en el establecimiento asistencial, una copia de resguardo debidamente certificada por sus autoridades, asentándose en el original y en la copia de resguardo los datos de los autos que motivan tal solicitud, el juzgado requirente y la fecha de remisión."* (Art. 19 Dec. 1089/2012).

Claro está desde ya, que el paciente - como, por su extensión y relación, los demás sujetos legitimados por la norma – tiene el derecho de acceder y solicitar copia de la historia clínica referida a él como a todos los datos que componen la misma.[5]

Operativamente con la registración de las historias clínicas en soporte papel tradicional y de otro tipo de impresos, lo que se efectuaba una vez requerida era una copia de la misma y por los mismos medios, copia impresa papel de dicho ejemplar. Este proceso resultaba dificultoso y continúa siéndolo, puesto que más allá de la centralización física de los registros en una sola institución o archivo, muchas veces esta era imperfecta y se debía volver a recoger la información de ciertos sectores, integrar los registros obtenidos, y recuperar aquellos pasibles de recuperación. Y también, muchas otras veces, aquella copia de resguardo que se creía íntegra no lo era en realidad.

Dada la informatización de las historias clínicas y la digitalización de aquellos estudios que antes únicamente resultaban impresos, la recuperación e integración de registros resulta exponencialmente más simple, y las idas y vueltas para obtener un registro completo de HCE se han reducido. El sistema tampoco es perfecto en todos sus supuestos, ya que como se ha mencionado, la parcialización de los registros en bases de datos que no se encuentran intercomunicadas de forma dinámica en muchas ocasiones produce la obtención de una copia parcial de HCE. Es dable destacar la obligación que pesa sobre las instituciones sanitarias de preservar una copia de resguardo de la HCE cuando ella fuere requerida judicialmente.

En cuanto al formato de la copia a obtener, las HCE pueden ser impresas como copiadas a formato digital, en cualquier soporte digital de capacidad suficiente que la contenga.

"El derecho fundamental a la autodeterminación informativa, como bien jurídico tutelado por el hábeas data, es un derecho autónomo, con una doble dimensión: sustancial, como derecho en sí mismo, esto es, con materialidad propia; e instrumental, es decir, como soporte para la cobertura protectiva de otros derechos, inter alia, los de intimidad, honor, dignidad. Tiene por objeto tutelar la información personal íntima y no íntima frente a su utilización incontrolada o disfuncional."[6]

La Ley de Derechos del Paciente regula en el Art. 20 el caso de negativa de entrega frente a la solicitud del paciente y que acciones puede tomar este[7], lo hace de este modo: *"Todo sujeto legitimado en los términos del artículo 19 de la presente ley, frente a la negativa, demora o silencio del responsable que tiene a su cargo la guarda de la historia clínica, dispondrá del ejercicio de la acción directa de "habeas data" a fin de asegurar el acceso y obtención de aquélla. A dicha acción se le imprimirá el modo de proceso que en cada jurisdicción resulte más apto y rápido. En jurisdicción nacional, esta acción quedará exenta de gastos de justicia."* (Art. 20 Ley 26529).

Por su parte, el Decreto Reglamentario fija en lo atinente sobre el Art. 19 que: *"Vencidos los plazos previstos en el artículo 14 de la Ley Nº 26.529 modificada por la Ley Nº 26.742 y esta reglamentación sin que se satisfaga el pedido, o evacuado el informe de la Historia Clínica éste se estimará insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en la Ley Nº 25.326, sin perjuicio de las sanciones que correspondan al establecimiento de salud respectivo."* (Art. 20 Dec. 1089/2012).

La doctrina ha dicho respecto de la acción constitucional de hábeas data[8]: *"Es sabido que actualmente la casi totalidad de las personas se encuentran registradas en un archivo, base o banco de datos y la evolución de las tecnologías modernas genera el tratamiento de la información colectada, que implica no sólo el almacenamiento sine die de los datos obtenidos, sino su relación, evaluación, bloqueo, destrucción, entrecruzamiento y cesión a terceros, con total y absoluto desconocimiento del titular de los datos personales.- La multiplicidad de secuelas y derivaciones de la actividad informática (1) —un verdadero fenómeno multifacético— desborda —reiteramos— el ámbito de la intimidad y privacidad de las personas, pues se afectan otros derechos, aunque resulta claro que ninguno de los mismos los abarca íntegramente y cada uno goza de características especiales, pues contienen individualmente elementos y presupuestos propios y se protegen conforme a determinadas agresiones y a tenor de diferentes consecuencias. - La protección de los datos personales configura una impronta real y jurídica, con características variadas, atendiendo a diversas manifestaciones, que deben ser consideradas especialmente para no frustrar su tutela; por ende, su garantía, el hábeas data, es un instrumento multidireccional que tiende a resguardar la siguiente pluralidad de derechos: a la intimidad, a la privacidad, a la autodeterminación informativa, a la verdad, a la identidad, al honor, al patrimonio, a la imagen, a la voz, a la información, y en definitiva, a la dignidad humana y consecuentemente, consideramos que aquélla debe funcionar como*

garantía instrumental polifuncional tendiente a tutelar los aludidos derechos."[9]

El paciente tiene el derecho de aceptar o rechazar tratamientos, terapias o procedimientos médicos o biológicos, con o sin expresión de causa, así como a revocar posteriormente su manifestación de la voluntad [10], "*para lo cual tiene derecho a tener la información necesaria y suficiente para la toma de su decisión, a entenderla claramente*"[11].

El Código Civil y Comercial establece al respecto del consentimiento informado para actos médicos e investigaciones en salud que el mismo es: *"… la declaración de voluntad expresada por el paciente, emitida luego de recibir información clara, precisa y adecuada, respecto a: a) su estado de salud; b) el procedimiento propuesto, con especificación de los objetivos perseguidos; ;c) los beneficios esperados del procedimiento; d) los riesgos, molestias y efectos adversos previsibles; e) la especificación de los procedimientos alternativos y sus riesgos, beneficios y perjuicios en relación con el procedimiento propuesto; f) las consecuencias previsibles de la no realización del procedimiento propuesto o de los alternativos especificados; g) en caso de padecer una enfermedad irreversible, incurable, o cuando se encuentre en estado terminal, o haya sufrido lesiones que lo coloquen en igual situación, el derecho a rechazar procedimientos quirúrgicos, de hidratación, alimentación, de reanimación artificial o al retiro de medidas de soporte vital, cuando sean extraordinarios o desproporcionados en relación a las perspectivas de mejoría, o produzcan sufrimiento desmesurado, o tengan por único efecto la prolongación en el tiempo de ese estadio terminal irreversible e incurable; h) el derecho a recibir cuidados paliativos integrales en el proceso de atención de su enfermedad o padecimiento….."* (Art. 59 CCy CNA).

La Ley de Derechos del Paciente, regula el instituto del "*consentimiento informado*"[12] en su capítulo III[13] , que define como: "*la declaración de voluntad suficiente efectuada por el paciente, o por sus representantes legales, en su caso, emitida luego de recibir, por parte del profesional interviniente, información clara, precisa y adecuada con respecto a: a) Su estado de salud; b) El procedimiento propuesto, con especificación de los objetivos perseguidos; c) Los beneficios esperados del procedimiento; d) Los riesgos, molestias y efectos adversos previsibles; e) La especificación de los procedimientos alternativos y sus riesgos, beneficios y perjuicios en relación con el procedimiento propuesto; f) Las consecuencias previsibles de la no realización del procedimiento propuesto o de los alternativos especificados; g) El derecho que le asiste en caso de padecer una enfermedad irreversible, incurable, o cuando se encuentre en estadio terminal, o haya sufrido lesiones que lo coloquen en igual situación, en cuanto al rechazo de procedimientos …."* Artículo sustituido por art. 2° de la Ley N° 26.742 B.O. 24/5/2012 (Art. 5 Ley 26529).

El consentimiento informado es entendido como un proceso, requerido con carácter general y obligatorio, salvo excepción legal, de toda actuación profesional en el ámbito médico-sanitario, y sólo puede ser otorgado por el paciente-consumidor de manera válida si este recibió la información sanitaria que permita otorgarlo.

El paciente tiene derecho a recibir la información sanitaria necesaria, es decir, adecuada a sus particulares circunstancias subjetivas, vinculada a su salud, como a no recibirla.[14]

El capítulo II de la Ley de Derechos del Paciente "*De la información sanitaria*", la define en el artículo 3° como "*aquella que, de manera clara, suficiente y adecuada a la capacidad de comprensión del paciente, informe sobre su estado de salud, los estudios y tratamientos que fueren menester realizarle y la previsible evolución, riesgos, complicaciones o secuelas de los mismos*" (Art. 3 Ley 26529). Esta información incluye por vía reglamentaria, las alternativas terapéuticas y sus riesgos y a las medidas de prevención, sus beneficios y perjuicios.

Debe ser brindada al paciente, y sólo podrá serle otorgada a terceras personas con autorización del mismo, salvo cuando exista el supuesto de incapacidad del paciente o imposibilidad de comprensión de la misma a causa de su estado físico o psíquico, supuesto en el cual será brindada a su representante legal o, en su defecto, al cónyuge que conviva con el paciente, o la persona que, sin ser su cónyuge, conviva o esté a cargo de la asistencia o cuidado del mismo y sus familiares hasta el cuarto grado de consanguinidad.

El derecho a la información genera la obligación legal en cabeza de los profesionales de la salud intervinientes, de brindarla a los pacientes o no, conforme la decisión expresa del paciente de no recibirla a los efectos de permitirles a estos un verdadero ejercicio de su autonomía de la voluntad, y como requisito previo y fundamental para la obtención del consentimiento informado.

La Ley de Derechos del Paciente en su Relación con los Profesionales e Instituciones de Salud establece como derecho del paciente en el Art. 2 Inc. F "*Información Sanitaria. El paciente tiene derecho a recibir la información sanitaria necesaria, vinculada a su salud. El derecho a la información sanitaria incluye el de no recibir la mencionada información."*.

El Decreto Reglamentario de la Ley de Derechos del Paciente terminó delineando los contenidos de la información sanitaria e introduciendo ciertas precisiones (Ej.: casos de incapacidad, salud pública en riesgo, estado de necesidad terapéutica).

El paciente tiene derecho a recibir la información sanitaria que a él se refiera por escrito, conforme al Art. 2 g) de la Ley 26529, a los fines de obtener una segunda opinión médica sobre su diagnóstico, pronóstico o tratamiento relacionados con su estado de salud. La reglamentación de este mismo artículo sigue estableciendo que el profesional tratante tiene al respecto un deber de colaboración, tomando en consideración la salud del paciente sobre cualquier condición; que el pedido y entrega de información a estos fines debe ser registrado en la historia clínica; que su entrega debe efectuarse por escrito; que el mismo profesional puede proponerla por razones de interés del paciente.

El cumplimiento adecuado del deber de información, es el requisito esencial e insoslayable del consentimiento informado, ya que sin información sanitaria adecuada, no puede haber consentimiento alguno. El basamento del deber de información son el

derecho del paciente de disponer libremente de su vida, salud e integridad física, su autonomía de la voluntad, y la asimetría informativa que adolece respecto del profesional al que acude.

Analizado el marco normológico que rodea la autonomía de la voluntad del paciente, resulta claro divisar que todo ello no sólo es aplicable por medio de la utilización de tecnologías de la información y la comunicación, sino que se multiplica en múltiples aspectos sus propias potencialidades.Las HCE deben incluir información relativa al paciente, al mismo tiempo que deben registrarse en ella los consentimientos informados del paciente, dos aristas que sostienen el arco de la autonomía de la voluntad del paciente. La utilización de bases de datos en los sistemas de salud permite y facilita el acceso dinámico a la información del paciente y sus consentimientos informados. En definitiva, en las HCE se puede volcar toda la información brindada al paciente.

Por otra parte, la implementación de sistemas inteligentes de HCE permitiría a su vez brindar información de modo más eficiente a todos los pacientes, generando respuestas de tipo cuasi automático, simplemente a confirmar por el médico. Ejemplo de ello sería que a un cúmulo de características determinadas por sistema le correspondiese ser brindada una serie de respuestas (información), y de ese modo se facilitaría la entrega de información particularizada al paciente y no simplemente la genérica. Del mismo modo, se podría utilizar el sistema de información hacia adentro, entendiendo por esto, el feedback dinámico que haría el sistema de información con la información recabada del paciente hacia el médico. Todo ello podría verse regulado normativamente a través de una disposición de carácter técnica-jurídica-sanitria.

Ello evitaría situaciones tales como la prescripción de medicamentos antagónicos o tratamientos incompatibles en el mismo paciente, si se tuviera información en tiempo real del mismo y a su vez las bases se encargaran de analizar conforme a parámetros cargados previamente y enviar alertas al médico las que serían transmitidas al paciente qué está sucediendo con el mismo y qué es lo que se debe informar.

Es más, la idea de ampliar el sistema de HCE a un cúmulo de bases de datos interconectadas e inteligentes, llegaría a los extremos de la búsqueda permanente en su sistema de relaciones de causalidad (Ej. ante la presencia de medicamento determinado, la modificación el algún sentido de un resultado de laboratorio daría un alerta automática, sin necesidad de consulta particular con el médico dada su causalidad probada y esperable; desde ya que luego del alerta, el médico procedería o no estimando como útil dicha información. Pero lo que se estaría alcanzando en miras a la preservación de la seguridad del paciente, es el acceso a la información dinámica que no se ve a medida que la misma ocurre y la prevención activa de daños en el paciente, sin tener que aguardar a la etapa de sus consecuencias.).

En este sentido, el Código de Ética de la Asociación Médica Argentina expresa al respecto de la utilización de los datos de salud y la instrumentación de registros electrónicos, prescripciones respecto a los fines de su utilización, el acceso a la información y su utilización, que encuentran arraigo en la Ley de Protección de Datos Personales y los principios que de ella emanan, en sus Artículos 226, 228 y 229 (entre ellas,

finalidad y calidad de los datos, legitimidad, seguridad, integridad, calidad técnica, anonimización, consentimiento, etc.)

3 Datos de Salud y sus Datos Relacionados

La calificación de dato sensible desde el punto de vista jurídico no es coincidente con la definición de sensibilidad técnica de un dato. Esto no resulta soslayable, cuando el marco normativo que se aplica a un campo de acción determinado (tratamiento informatizado de datos) introduce terminología homónima para conceptos disímiles, obligatoria para sujetos que deberán manejar dos estándares (jurídico-técnico) disímiles.

Es sabido que el dato de salud como categoría de dato, entraña una sensibilidad inseparable a su esencia, ya sea que identifiquemos la misma con la posibilidad de discriminación que engendra[15], o más acertada y modernamente, con su carácter personalísimo y la posibilidad que acarrea para su titular en el ejercicio de sus derechos más personalísimos (autonomía de la voluntad, realización de su proyecto de vida, autodeterminación informativa, libertad, intimidad, privacidad, seguridad, no discriminación, etc.).

No obstante ello, en el ámbito de salud no es excluyente. Los datos de salud no son los únicos que merecen protección crítica en su tratamiento y procesamiento, al igual que en todas las tareas – por más ínfimas que estas sean – que se realicen sobre los mismos de manera rutinaria.

Tomemos de ejemplo para graficarlo, el hecho de laboratorio en el que poseemos una clínica que se encuentra exclusivamente dedicada al tratamiento de una patología determinada. Aún antes que cualquier dato de salud, resulta un dato sensible el sólo conocimiento de que alguien ingresó a ese lugar, puesto que con datos mundanos se pueden deducir “otros datos” sensibles o datos de otro tipo cuyo procesamiento pueda resultad sensible. En este ejemplo, el dato no es nada más ni nada menos que un simple hecho, que procesado y relacionado se convierte en un dato sensible, que sirve para perfilar una determinada situación de salud en un individuo potencialmente identificable por medio de otros datos de simple acceso y percepción.

Es por ello que la Ley debiera mantener una congruencia y uniformidad terminológica con el campo de realidad técnica al cual accede y regula, en el que abunda la interconexión informativa. El concepto vigente de dato sensible enfocado en criterios restrictivos no permite establecer un concepto técnico de sensibilidad que trascienda sus propias limitantes. El concepto de dato sensible debiera perfeccionarse por medio del aporte interdisciplinario técnico-jurídico, con miras a la complementariedad regulatoria del régimen vigente de privacidad de datos, a través de la reinvención terminológica de ciertas categorías y la introducción estandarizada de procesos de manipulación de datos técnicamente actualizados y eficaces e instrumentos de seguridad de datos con teleología preventiva.

Dato sensible para la práctica técnica refiere a cualquier dato cuya utilización per se o en combinación con otros, por fuera de los fines legítimos y autorizados de tratamiento informatizado, pueda devenir en dañina para su titular, motivo por el cual se lo trata o procesa con especial cuidado, seguridad y con independencia absoluta respecto del contenido de su información o de aquello que pueda llegar a revelar.

Es decir, en la práctica técnica y económica del tratamiento informatizado de datos no se relaciona al "dato sensible" con la cualidad per se del dato o su caracterización, como lo hace la Ley de Protección de Datos Personales, sino con el tratamiento ilegítimo del que pueda ser objeto.

El dato sensible en el tratamiento informatizado, bien puede referir a una información tanto pública y accesible como privada y reservada, cualquiera fuere su temática, y alude a la utilización "sensible" como sinónimo de riesgosa, que un extraño pueda derivar o inferir de ese dato.

La coexistencia de estas dos definiciones para el mismo vocablo suscita en la práctica un sinnúmero de problemas y desajustes, que conforman el universo de problemas puntuales que derivan del tratamiento informatizado de datos.

Para proteger al titular de los datos personales "sensibles" técnicamente, se debe recurrir a una definición amplia de dato sensible que no apunte a las características de su categoría sino a las consecuencias que pudieran surgir de su incorrecto tratamiento, las que justificarían el grado de seguridad aplicable en el tratamiento informatizado del mismo.

En síntesis y progresando, la definición de dato sensible en el tratamiento informatizado de datos no posee una finalidad estrictamente académica sino netamente práctica; sirve para justificar el tratamiento seguro del dato y sus relacionados, con independencia de las características de su contenido y la información que el mismo revele.

El tratamiento sensible del dato, técnica y jurídicamente, significaría la realización de procedimientos sobre la información de las personas, que permitan unir elementos conducentes a la identificación de contenido único o relacionado que facilite el uso ilegítimo de dichos datos. Esto último procedería finalmente a verificarse en cada supuesto particular contemplado y donde la respuesta de ello resultase afirmativa, probada la relación de causalidad devenida de dichos procedimientos, se procedería a responsabilizar al depositario del dato sujeto al tratamiento informatizado fallido, dando solución jurídica al conflicto suscitado.

La importancia de la protección de estos "datos sensibles", en virtud de la nueva categorización que se propone de tipología abierta, redundaría en su sensibilidad entendida como capacidad de producir daños o potencialidad dañosa consecuencia de su mal procesamiento o descuidado depósito. La sensibilidad de un dato dependerá exclusivamente del contexto específico de su tratamiento.

4 Protección Técnica de los Datos de Salud y sus Relacionados

En lo referente a la opción de protección de los datos técnicamente sensibles, la norma hasta el momento se ha pronunciado en pos de la técnica de encripción. Sin embargo, y a pesar de que la encripción constituye una técnica adecuada para la protección y seguridad de datos bajo resguardo o traslado, no es la única ni la más idónea o plausible para todos los supuestos.

La encripción generalizada conlleva un altísimo costo que no todas las organizaciones son capaces de afrontar, al mismo tiempo que no se erige como la más idónea y estandarizable para todo supuesto, específicamente y en lo que la ley nada dice, al respecto del uso de estos datos para prueba de aplicativos y la construcción de ambientes seguros de testeo y por otro lado su uso en la construcción de bases de datos para explotación analítica.

La encripción estandarizada no se encuentra como una de las vías más adecuadas para facilitar el procesamiento de datos contenidos en historias clínicas, a simple vista se trasluce como un costo que no podrán enfrentar numerosas instituciones de salud, no siendo económico tampoco resulta del todo eficiente. Si bien es una más de las técnicas disponibles, esta puede complementarse y utilizarse en conjunto con otro abanico de técnicas que cumpliendo los objetivos jurídicos de tutela, se adaptan de manera más flexible a las tareas técnicas que demanda el procesamiento diario de datos en el seno de una institución sanitaria.

Cabe aclarar que la encripción, como toda otra técnica ordenada de cifrado, al ser un procedimiento matemático reversible por métodos estandarizados y conocidos, tampoco garantiza absoluta y perdurable seguridad de los datos protegidos. Es por ello que se justifica la utilización combinada de un conjunto de técnicas que permitan un más elevado y perdurable nivel de seguridad de los datos.

El presente trabajo propone la introducción de la práctica que aquí se indicará como “protección técnica de los datos”, cuyo principio rector será la práctica de utilización de datos, transporte y conservación de los mismos privados de elementos identificatorios y referenciales de la persona tutelada por la norma. El esquema que se propone es la utilización de la información una vez sustituidos los elementos identificatorios y referenciales manteniendo la morfología de dicha información y su capacidad de procesamiento.

La idea que se procura introducir en el presente es la de un cambio de modelo de base del uso de los datos identificatorios y referenciales en la actividad del procesamiento y tratamiento informatizado de los mismos; sin la necesidad de realizar cambios en el mercado actual, puesto que el resultado final obtenible en términos de mercado sería el mismo, pero evitando exponer al sujeto en los análisis previos conservando sus características de interés comercial luego de la pertinente protección de sus datos técnicamente sensibles.

La protección como proceso técnico importaría, tanto el ocultamiento de los datos técnicamente sensibles a través de diversos procesos técnicos que se citarán más ade-

lante, como la implementación de técnicas de ocultamiento de formatos conocidos en el depósito en que son guardados a los fines de su explotación analítica. Nuestra ley debiera considerar estos tecnicismos que resultan fundamentales al momento de materializar una adecuada, más no lírica, seguridad de datos.

El "layout" o diseño del registro de la información, entendido como el modo y esquema por medio del cual se dispone, posiciona y distribuye la información, debiera acompañar el registro de los datos y conformar parte, también, del objeto de protección de datos; en el caso se propone la protección del "layout" en el que se disponen las HCE.

El "layout" de los distintos archivos que componen una HCE tiene la virtualidad de revelar posicionamiento y morfología de datos sensibles técnicamente, características éstas que son la vía más directa de encuentro y reconocimiento del dato protegido. Es por ello que se debe evitar, proteger y penalizar también esta facilitación de acceso al dato por intermedio de la filtración del "layout" de cualquier base de datos. Sintéticamente en relación a esto último, se debiera asociar y asimilar el "layout" de los datos a la caracterología de la protección de datos técnicamente sensibles.

Estos nuevos estándares de protección en el régimen de privacidad de datos redundarían indirectamente en la disminución de costos por el cumplimiento adecuado de regulaciones, bajo una visión superadora de estas últimas, y focalizada en una premisa de eficiencia económica a la inversión en la protección y seguridad de datos.

Otro beneficio formidable de estas prácticas propuestas se condensaría en la reducción exponencial del riesgo operacional y de responsabilidad legal asociado a la privacidad de los datos, y en particular en el caso de las historias clínicas, del mantenimiento de su virtualidad como elemento probatorio no vulnerable.

Finalmente, se pueden citar como otras ventajas de índole preventiva que trascienden la simple firma de acuerdos de confidencialidad – los cuales han demostrado a lo largo del tiempo una baja efectividad-, la facilitación de prácticas de auditoría, la mejora de la calidad y los tiempos de respuesta frente al acaecimiento de contingencias de seguridad, y el incremento de la trazabilidad y capacidad de detección de actividades sospechosas internas y externas.

El manejo de información debiera, dentro de los parámetros que aquí se proponen, restringir y minimizar al máximo el acceso a los datos técnicamente sensibles, específicamente en las tareas de testeo de aplicaciones, para las cuales se sugiere la extracción de lotes adecuados de datos que hayan sido previamente protegidos.

Finalmente, como resultado de esta organización se obtendrían beneficios inmediatos al poder asociar los lotes de datos originales productivos y contenedores naturales de información sensible de tipo técnico y personalísimo a áreas de almacenamiento a las que solo acceden los aplicativos autorizados durante su ejecución, mientras que los lotes de información de idéntica morfología pero reducidos en cantidad a través de criterios inteligentes de selección y protegidos serían accedidos libremente por todo el personal de desarrollo y testeo y otros terceros sin que esto implique poner en riesgo el fin buscado que es el de la protección de la privacidad de los datos.

En los tiempos que corren y en virtud del vertiginoso desarrollo tecnológico, es hora de buscar soluciones prácticas y adaptativas a esta realidad que no posean el indeseado efecto colateral de frenar, disminuir, reversar y/o desalentar los progresos en ese ámbito. Máxime cuando la generalización de la utilización de las HCE viene dada por ley, y la HCE es una herramienta fundamental para la medicina de nuestros tiempos, l que ha facilitado y mejorado – aún a pesar de sus presentes defectos – la práctica médica diaria y la terrible y hasta trágica contingencia de la descentralización de la información del paciente.

El derecho en el área de las nuevas tecnologías puede colaborar en el régimen de regulación de la privacidad de datos brindando respuestas preventivas como la que aquí se propone, disminuyendo y previniendo la ocurrencia de dañosidad en este campo.

5 Tratamiento Informatizado de Datos de Salud – E-token

Resulta innegable la utilidad que representa hoy día, en el área sanitaria, la posibilidad de procesar informáticamente los datos de salud, ya sean estos operativos o administrativos y en particular todo aquel que se integre al registro de la historia clínica de cada paciente. En cada caso de implementación particular de estas técnicas, su integración y desarrollo es a medida, y en la actualidad no existe al momento, a nivel nacional, un sistema centralizado ni un estándar operativo jurídicamente exigible respecto de la modalidad a elegir para la implementación de las HCE – y se puede arriesgar a decir tal vez jamás exista -.

Sin perjuicio de este panorama de descentralización y atomización en el que priman las implementaciones privadas, particulares o públicas locales, a nivel individual de cada organización, todas estas implementaciones buscan como meta primaria la mejora continua en la atención del paciente. No obstante, ello no es fácil cuando constantes amenazas a la seguridad en el tratamiento de datos de salud afectan a este último, quien se ve expuesto a riesgos y daños posiblemente evitables desde lo técnico, con condiciones de operatividad exigibles e implementables desde lo jurídico.

En líneas generales los problemas que más afectan en el ámbito sanitario el tratamiento informatizado de datos de salud son: la inexistencia de una garantía de interoperabilidad de los sistemas utilizados en la atención del paciente, la ausencia de un plan de registro de salud durable y perdurable para toda la vida del paciente, la obsolescencia programada de los sistemas y del equipamiento utilizado para soportarlos, la coexistencia en un mismo ámbito sanitario de múltiples culturas médicas, la falta de cooperación con el cambio, defectos de capacitación, y fallas de comunicación entre las demandas de las diferentes áreas que competen la atención del paciente, entre otras problemáticas que se podrían mencionar.

Dicho todo esto, es destacable que a nivel jurídico no se han abordado seriamente estas últimas, ya sea en cuerpos normativos centralizados o en varios cuerpos normativos independientes referidos a la misma temática.

Este hecho es observable con sólo acudir a la lectura del Art. 13 de la Ley de Derechos del Paciente, norma que se encarga exclusivamente de la regulación de los derechos del paciente, la historia clínica y el consentimiento informado, el que reza al respecto de la HCE "*Historia clínica informatizada. El contenido de la historia clínica, puede confeccionarse en soporte magnético 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. 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. - La reglamentación establece la documentación respaldatoria que deberá conservarse y designa a los responsables que tendrán a su cargo la guarda de la misma."*

La respectiva reglamentación de dicho artículo, efectuada por el decreto 1089/2012, establece a su vez *"Historia clínica informatizada. La historia clínica informatizada deberá adaptarse a lo prescripto por la Ley Nº 25.506, sus complementarias y modificatorias.- La documentación respaldatoria que deberá conservase es aquella referida en el artículo 16 de la Ley Nº 26.529 modificada por la Ley Nº 26.742, que no se pueda informatizar y deberá ser resguardada por el plazo y personas indicados en el artículo 18 de esa misma ley."*.

Sin intenciones de ahondar en dicho análisis *brevitatis causae*, cabe sólo mencionar respecto de esto último el claro ejemplo de una de las problemáticas citadas, ya que aquí es la norma la que manda a implementar un recurso técnico jurídico que aún hoy en día no tiene implementación generalizada a nivel nacional, a saber, la firma digital. En su caso y conforme a los mismos términos que utiliza la Ley 25506, ante la implementación de un artilugio técnico semejante, se estará requiriendo de la utilización de firma electrónica, técnica que – conforme al idéntico razonamiento efectuado respecto de la técnica de encripción y siendo una de ellas – no es la única ni mejor técnica de seguridad o resguardo utilizable en la implementación de las HCE, bien se podrían utilizar otras.

Como ya se venía diciendo en los segmentos anteriores, una de las piedras basales en las que se edifica la infraestructura de HCE, cualquiera sea la institución, su administración, magnitud y operatoria, son la seguridad y confidencialidad de los datos de salud de los pacientes, usuarios de los mismos y a su vez, usuarios de las bases de datos que contienen sus datos de salud.

En concordancia con lo propuesto respecto de la "protección técnica de datos", se suma a ello la idea de implementar jurídica y técnicamente la exigencia de la portabilidad de e-token del paciente relacionado unívocamente con su HCE y de cada integrante de la organización sanitaria para permitir acceso a los sistemas y de la implementación de un sistema de control de cambios y alertas - análogo a los que se utilizan en la industria bancaria y financiera -, lo que le permitiría al paciente un más adecuado control de la información contenida en la misma en su tratamiento informatizado. Con ello se cumpliría el requisito que ordena la norma respecto de garantizar en las HCE "*accesos restringidos con claves de identificación"*.

Los dispositivos token generan códigos que se modifican de manera constante, sin reiteración, y se pueden utilizar en todas las operaciones que se realizan sobre las HCE, ya sea por parte de los pacientes como del personal médico, administrativo, etc. Cada sujeto al tener un generador propio quedará identificado en la operatoria que realice y cada operación efectuada en las HCE tendrá su marca e identificación inequívoca de origen, tiempo y lugar. Por ejemplo, si el paciente se encuentra en consulta con el médico, el resumen del encuentro será firmado con la clave de ambos; si el médico ingresara a modificar o añadir algún dato a la HCE del paciente, dichos cambios serán indicados – es decir, sin sobreescritura del contenido anterior – y firmados por el médico; lo mismo sucedería respecto de la actividad administrativa operada en el registro único del paciente en la institución; etc. Esto último refiere al requisito enunciado por el Artículo 13 citado, el que manda a adoptar respecto de las HCE un "*control de modificación de campos o cualquier otra técnica idónea para asegurar su integridad"*

Otro ámbito de mejora por medio de los e-token, será el de las transferencias seguras de información entre diferentes puntos de la organización con consentimiento del paciente (Ej.: entre áreas, servicios, de hospital a consultorios relacionados, etc.)

Por lo tanto, se podrían optimizar los niveles la seguridad y la inviolabilidad de las HCE, resguardando a su vez la intimidad y confidencialidad por medio de la complementariedad de estos cambios con la implementación y exigencia de claves de seguridad diferenciadas que permitan el acceso a diversos niveles de datos y sistemas de registro de acceso, que almacenen todas las transacciones y flujos de datos (Ej.: administración no ve datos de diagnóstico, accede sólo a datos necesarios para su actividad; desarrolladores acceden a datos protegidos para realizar sus pruebas; etc.).

Los sistemas de HCE y aquellos en los que se traten datos relacionados a los mismos deben respetar el derecho ético y legal de cada paciente, a su privacidad, intimidad, confidencialidad y autodeterminación informativa.

6 Plataforma de Comunicación

La Ley de Derechos del Paciente, en conformidad con el historial de desarrollos doctrinarios efectuados en la materia, caracteriza en su Artículo 12 a la HC como un documento "*cronológico, foliado y completo en el que conste toda actuación realizada al paciente por profesionales y auxiliares de la salud*", del que forman parte "*los consentimientos informados, las hojas de indicaciones médicas, las planillas de enfermería, los protocolos quirúrgicos, las prescripciones dietarias, los estudios y prácticas realizadas, rechazadas o abandonadas, debiéndose acompañar en cada caso, breve sumario del acto de agregación y desglose autorizado con constancia de fecha, firma y sello del profesional actuante*" (Artículo 16 – Integridad).

En lo atinente al requisito de "*unicidad*" de la HC, la norma dice "*La historia clínica tiene carácter único dentro de cada establecimiento asistencial público o privado,*

y debe identificar al paciente por medio de una "clave uniforme", la que deberá ser comunicada al mismo" (Artículo 17).

Una de las problemáticas más habituales que enfrentan las instituciones sanitarias en la gestión diaria de las HCE, es la descentralización de la información disponible del paciente en todo lugar y momento. En ellas es observable que la mentada "unicidad" que por ley se define, se alcanza al unificar los registros a través del identificador único (clave uniforme) del paciente cuando se archiva o acumula la documentación de la HC en su registro (sea esta nativamente electrónica o digitalizada), y no cuando se consulta dinámicamente esta información. Ejemplo típico de ello resulta en el epítome que grafica el paciente receptor de indicaciones contradictorias o incompatibles por parte de médicos de diversos servicios dentro de la misma institución, quienes si bien consultan el mismo sistema centralizado, no pueden acceder ni consultar toda la información centralizada y compilada del paciente en tiempo real.

Sintéticamente se puede decir que la información del paciente se encuentra dividida en segmentos parciales, que luego integran la HCE única del mismo, y que estos últimos residen en lugares dispares e inaccesibles de manera directa, los que adolecen de interoperabilidad dinámica.

La falta de interoperabilidad se resume en el hecho que los segmentos parcializados de información del paciente que contiene el sistema cerrado de HCE de la institución sanitaria, se encuentran depositados y son procesados en una amplia variedad de bases de datos hospitalarias incompatibles entre sí e incomunicadas.

Por todo ello se concluye que el defecto crónico que sufren las plataformas de comunicación en la implementación de las HCE a nivel técnico impacta de forma directa en la esencia jurídica documental de la HCE.

Estos defectos propios de la infraestructura de HCE, su arquitectura desorganizada y promiscuamente planificada, la tornan a veces desajustada en materia de desempeño, e incierta y aún cuestionable en materia de transparencia funcional e informativa.

Para concluir, los sistemas de HCE deben ser lo más abiertos posibles y sus plataformas capaces de servir a diversos tipos de información, servicios y medios de comunicación, siendo esto último planificado estratégicamente teniendo en particular consideración la operatoria de la institución sanitaria a la cual accede.

7 Conclusiones

Dada la práctica generalizada de implementación de sistemas de HCE en las instituciones sanitarias, se debe efectuar un replanteo y abordaje serio tanto, desde lo jurídico como de lo técnico de manera conjunta, respecto de la temática de procesamiento de datos, sean estos datos de salud, personales, sensibles o relacionados, por la importancia y la magnitud de los derechos involucrados en juego.

Se debe reconocer como un hecho que el sistema jurídico de protección de datos vigente no puntualiza una desconfianza natural formada sobre la protección de datos, es decir, no tutela activa, dinámica ni preventivamente los datos en todas aquellas tareas rutinarias que se efectúan dentro de la actividad lícita y reglamentaria misma que implica su tratamiento informatizado en todo el ciclo de vida del mismo, y por lo tanto resulta inadecuado a los fines de alcanzar un elevado y admisible grado de protección respecto de los datos que contienen las HCE y aquellos que se procesan informatizadamente en la atención del paciente (sean datos de salud, personales o relacionados).

Respecto de esto último, cabe reiterar como se ha dicho previamente que para proteger al titular de los datos personales "sensibles", se debe recurrir a una definición amplia de dato sensible que no apunte a las características de su categoría sino a las consecuencias que pudieran surgir de su incorrecto tratamiento, las que justificarían el grado de seguridad aplicable en el tratamiento informatizado del mismo; y que en lo referente a la opción de protección de los datos técnicamente sensibles, la norma hasta el momento se ha pronunciado en pos de la técnica de encripción, que no es la única ni la más idónea o plausible para todos los supuestos.

La propuesta que se resume del presente trabajo redundaría en que la protección como proceso técnico importaría, tanto el ocultamiento de los datos técnicamente sensibles a través de diversos procesos técnicos no productivos, como la implementación de técnicas de ocultamiento de formatos conocidos en el depósito en que son guardados a los fines de su explotación analítica o estadística.

Los basamentos sobre los que se edifican las implementaciones de sistemas de HCE, tanto desde lo técnico, práctico y jurídico, son la seguridad y confidencialidad que se debe garantir al paciente. Por ello se propone a su vez la utilización de dispositivos e-token, para cumplir el requerimiento de accesos restringidos con claves de identificación que exige adecuadamente la Ley de Derechos del Paciente.

Por último resta mencionar las problemáticas prácticas y operativas que constituyen la falta de interoperabilidad y comunicación en la implementación de sistemas de HCE, que afectan los caracteres de integralidad y unicidad del documento HC y atentan contra su correcto funcionamiento, a cuyos efectos se sugiere la planificación estratégica de su servicio, tomando en consideración las especificidades de la operatorio interna de cada institución sanitaria.

Referencias

[1] GARAY, Oscar Ernesto: La ley 26.529 de Derechos del Paciente en su relación con los Profesionales e Instituciones de la Salud. Publicado en: DFyP 2010 (enero-febrero), 01/01/2010, 165. AR/DOC/4615/2009.

[2] AIZENBERG, Marisa ROITMAN, Adriel J.: Los derechos de los pacientes y su reconocimiento a nivel nacional. Publicado en: LA LEY 29/12/2009, 29/12/2009, 1 - LA LEY2010-A, 826. AR/DOC/4541/2009

[3] GARAY, Oscar Ernesto MADIES, Claudia Viviana: La reglamentación de la ley 26.529 confirma paradigmas favorables a los pacientes. Publicado en: DFyP 2012 (septiembre), 01/09/2012, 180. AR/DOC/4358/2012.

[4] ALBANESE, Susana J.: Relación médico-paciente: el derecho a informar y el acceso a la historia clínica. Publicado en: LA LEY1990-E, 248 - Responsabilidad Civil Doctrinas Esenciales Tomo V, 01/01/2007, 251. AR/DOC/11585/2001.

[5] AIZENBERG, Marisa ROITMAN, Adriel J.: El nuevo régimen de titularidad y guarda de la historia clínica. Publicado en: DFyP 2010 (mayo), 01/05/2010, 190. AR/DOC/2163/2010.

[6] BAZÁN, Víctor: "El hábeas data como proceso constitucional autónomo. Protección del derecho a la autodeterminación informativa". Publicado en: LA LEY 21/11/2012, 21/11/2012, 1 - LA LEY21/11/2012, 1 - LA LEY2012-F, 1052.

[7] BARRAZA, Javier Indalecio: Historia clínica. Su incidencia en la responsabilidad médico profesional, breve análisis de la importancia del citado documento. Publicado en: LA LEY2000-A, 1171. AR/DOC/18116/2001.

[8] *Véase*:

MOLINA QUIROGA, Eduardo: Derecho a la información de la salud y hábeas data específico. Derechos esenciales del paciente. LA LEY 26/08/2013, 26/08/2013, 1 - LA LEY2013-E, 609; AR/DOC/1398/2013.

LÓPEZ MIRÓ, Horacio G.: ¿Qué hacer ante la negativa del médico a entregar la historia clínica? Publicado en: DJ20/12/2006, 1210.

GOZAÍNI, Osvaldo Alfredo: "Hábeas Data. Protección de Datos Personales" 2° Edición Ampliada y Reformada. Editorial Rubinzal-Culzoni. Buenos Aires, 2011.

GILS CARBÓ, Alejandra M.: "Régimen Legal de las Bases de Datos y Hábeas Data". Editorial La Ley. Buenos Aires, 2001.

CESARIO, Roberto: "Hábeas Data. Ley 25326". Editorial Universidad. Buenos Aires, 2001.

CIFUENTES, Santos E. (h.): El derecho a los datos personales y el habeas data. Publicado en: Acad.Nac. de Derecho 2008 (mayo), 01/01/2008, 1. AR/DOC/2104/2008.

COLERIO, Juan Pedro: El secuestro de la historia clínica como diligencia preliminar ¿es una medida preparatoria o conservatoria? Publicado en: LA LEY1996-E, 286 - Responsabilidad Civil Doctrinas Esenciales Tomo V, 01/01/2007, 661. AR/DOC/9141/2001.

COMPAGNUCCI DE CASO, Rubén H.: La responsabilidad médica y la omisión en la presentación de la historia clínica. Publicado en: LA LEY1995-D, 549 - Responsabilidad Civil Doctrinas Esenciales Tomo V, 01/01/2007, 641. AR/DOC/13278/2001.

CORNET, Manuel: Valor de la Historia Clínica en los juicios de mala praxis Médica. Publicado en: RCyS2008, 319. AR/DOC/2914/2008

CROVI, Luis Daniel: "Los daños ocasionados por el uso indebido de datos personales en Internet". Publicado en: RCyS2008, 330.

DE FALCO, Carlos Rodolfo: Enfoque Pericial. La historia clínica como herramienta idónea para reflejar la praxis médica. Publicado en: DJ2005-1, 1071. AR/DOC/727/2005.

[9] MASCIOTRA, Mario: "El controvertido ámbito de aplicación de la ley de protección de datos personales". Publicado en: LA LEY 29/02/2008, 29/02/2008, 3 - LA LEY2008-B, 166.

[10] Ley 26529 Art. 2 e)

[11] Decreto 1089/2012 Art. 2 e)

[12] Ver LÓPEZ MESA, Marcelo J.: Pacientes, médicos y consentimiento informado. LA LEY 26/02/2007, 26/02/2007, 1 - LA LEY2007-B, 867 - Responsabilidad Civil Doctrinas Esenciales Tomo V, 01/01/2007, 619: "…Partimos en este tema del sobreentendido de que la expresión "consentimiento informado" no es precisamente la mejor que puede utilizarse para referirse a la autorización del paciente a que se le practique un tratamiento médico sugerido por el galeno.

Para dicho acto del paciente existen nombres más técnicos y adecuados, como podrían ser "asentimiento del paciente" o aún "autorización al tratamiento"; o "consentimiento esclarecido", que utiliza la Corte de Casación francesa…"

13 Ley 26529 Art. 5º

[14] *Véase*: FERREYRA, María Inés: La obligación de información. RCyS2014-I, 17. Cita Online: AR/DOC/4512/2013: "…La información permite que el paciente ejercite una serie de derechos personalísimos relacionados con sus ideales, su libertad, creencias religiosas, integridad física o psíquica. El fundamento está en el desnivel cognoscitivo que existe entre el paciente y el profesional de la salud. Al informar el médico al paciente, esta desigualdad y desequilibrio se morigeran, y el paciente dispone de una herramienta de control para limitar el poder del experto…."

[15] *Véase*:

MOLINA QUIROGA, Eduardo, Los datos de salud en la ley 25.326 de Protección de Datos Personales, SJA 28/4/2004.

TRAVIESO, Juan Antonio MORENO, María del Rosario: "La protección de los datos personales y de los sensibles en la ley 25.326". Publicado en: LA LEY 14/07/2006, 14/07/2006, 1 - LA LEY2006-D, 1151.