Revista Científica de UCES
Vol. 29 N° 1 (Enero - Julio de 2024)
ISSN Electrónico: 2591-5266
(pp. 1-41)

La protección de los Datos Sensibles del Paciente, en la Historia Clínica Electrónica a la Luz de los Principios de la Ética Biomédica y las Orientaciones de la OMS[1]

Maria Belen Nadal[2]

https://orcid.org/0009-0000-9156-8061

mariabelennadal@live.com

Fecha de Recepción: 3 de abril de 2024

Fecha de Aceptación: 17 de abril de 2024

ARK/CAICYT: https://id.caicyt.gov.ar/ark:/s25915266/b9qpvu3x9

RESUMEN

En el presente trabajo hemos estudiado los derechos del paciente, a la luz del marco normativo vigente y de los principios de la ética biomédica, por cuanto recientemente ha sido sancionada la ley de Historia Clínica Electrónica en Argentina, y nos preocupa que la confidencialidad de los datos sanitarios pueda afectarse si no se respetan estos principios, y los protocolos de seguridad legales e informáticos mínimos e indispensables.

Nuestra hipótesis es que en Argentina aún no se encuentran garantizadas las condiciones mínimas de seguridad informática para evitar la afectación de los derechos del paciente. Por ello es

[1] Artículo original aceptado para su publicación el día 17 de abril de 2024.

[2] Abogada. Doctoranda en Derecho, UCES. Diplomada en Derechos de Personas con Discapacidad, Pontificia Universidad Católica de Perú. Mediadora especialista en Mediación Penal y Justicia Restaurativa, Aso. Argentina de Mediación. Miembro de la Asociación Argentina de Profesionales de la Salud Mental. Profesora de posgrado de la Univ. Nacional de San Luis. Docente en Univ. De Congreso, Mendoza. Conferencista en congresos nacionales e internacionales desde el año 2012 a la actualidad en materia de salud mental y discapacidad.

importante que nos preguntemos ¿Cuáles principios éticos y normativas vigentes deben respetarse en la historia clínica electrónica? Asimismo ¿Cuáles son los riesgos que deben evitarse? Pues bien, en el presente artículo hemos intentado dar respuesta a ello.

Para este trabajo hemos elegido un tipo de diseño no experimental, donde hemos analizado los principios éticos y el marco normativo. Asimismo, el alcance de la investigación es descriptiva y según su propósito es básica. El abordaje de investigación es combinado cualitativo y cuantitativo, del tipo modelo de esquema dominante cualitativo.

ABSTRACT

In the present work we have studied the rights of the patient, in light of the current regulatory framework and the principles of biomedical ethics, since the Electronic Medical Record law has recently been sanctioned in Argentina, and we are concerned that the confidentiality of the Health data may be affected if these principles, and the minimum and essential legal and computer security protocols, are not respected.

Our hypothesis is that in Argentina the minimum computer security conditions are not yet guaranteed to avoid affecting patient rights. Therefore, it is important that we ask ourselves: What ethical principles and current regulations must be respected in the electronic medical record? Likewise, what are the risks that should be avoided? Well, in this article we have tried to answer this.

For this work we have chosen a type of non-experimental design, where we have analyzed the ethical principles and the regulatory framework. Likewise, the scope of the research is descriptive and according to its purpose it is basic. The research approach is combined qualitative and quantitative, of the qualitative dominant schema model type.

RESUMO

No presente trabalho estudamos os direitos do paciente, à luz do atual marco regulatório e dos princípios da ética biomédica, uma vez que a lei do Prontuário Médico Eletrônico foi recentemente sancionada na Argentina, e nos preocupa que a confidencialidade do Registro Médico os dados podem ser afetados se estes princípios e os protocolos legais e de segurança informática mínimos e essenciais não forem respeitados.

Nossa hipótese é que na Argentina ainda não estão garantidas as condições mínimas de segurança informática para evitar afetar os direitos dos pacientes. Portanto, é importante que nos perguntemos: Quais princípios éticos e normas vigentes devem ser respeitados no prontuário eletrônico? quais são os riscos que devem ser evitados? Bem, neste artigo tentamos responder a isso.

Para este trabalho optamos por um tipo de desenho não experimental, onde analisamos os princípios éticos e o marco regulatório. Da mesma forma, o escopo da pesquisa é descritivo e conforme sua finalidade é básico. A abordagem da pesquisa é combinada qualitativa e quantitativa, do tipo modelo de esquema qualitativo dominante.

Introducción

En el presente trabajo presentamos un profundo análisis sobre la flamante ley de Historia Clínica Electrónica en Argentina, desde el paradigma ético y asimismo abordando todo el marco normativo necesario para entender su correcto tratamiento, en aras de promover el respeto por los derechos del paciente. Para ello hemos estudiado los principios de la ética biomédica, como así también el derecho positivo argentino que consagra derechos humanos fundamentales en materia de salud. Además nos pareció sumamente importante el documento de la Organización Mundial de la Salud, emitido en enero de este año, sobre Ética y Gobernanza en materia de inteligencia artificial para cuestiones de Salud, donde realizó más de 40 recomendaciones a los gobiernos para su correcto tratamiento.

Consideramos oportuno recordar que nuestro país aún no cuenta con la implementación cabal de este sistema, por lo cual es el momento para hacernos un replanteo de las falencias en materia de seguridad informática que presentan los sistemas actuales de recolección y tratamiento de datos sanitarios, como la falta de capacitación a los profesionales de la salud y a los demás actores que intervienen en el acceso y manipulación de los registros electrónicos sanitarios.

Sabemos que en un centro de salud, no sólo es el médico quien ingresa a la base de datos que contiene la información del paciente, sino hasta el personal administrativo que tiene a su cargo la carga de turnos, facturaciones, estudios y prácticas.

Nuestra hipótesis es que en Argentina aún no se encuentran garantizadas las condiciones mínimas de seguridad informática para evitar la afectación de los derechos del paciente. Por ello es importante que nos preguntemos ¿Cuáles principios éticos y normas vigentes deben respetarse en la historia clínica electrónica y cuáles son los riesgos que deben evitarse?

Para este trabajo hemos elegido un tipo de diseño no experimental, donde hemos analizado los principios éticos y las leyes vigentes en la materia. Asimismo, el alcance de la investigación es descriptiva y según su propósito es básica. El abordaje de investigación es combinado cualitativo y cuantitativo, del tipo modelo de esquema dominante cualitativo.

Desarrollo

En este apartado abordaremos nuestro análisis en tres partes, primeramente estudiaremos el marco normativo vigente en materia de derechos del paciente e historia clínica electrónica en Argentina posteriormente analizaremos los principios de la ética biomédica que deben regir en el tratamiento de la información, para finalmente hacernos eco de las recomendaciones realizadas por la OMS para el tratamiento de cuestiones de salud mediante inteligencia artificial y considerar las adecuadas para la historia clínica electrónica en nuestro país. Todo ello atendiendo al principio básico de la autonomía del paciente y haciendo de ello nuestro eje de referencia.

Marco Normativo

Si partimos del marco normativo existente previo a la ley de Historia Clínica Electrónica, podremos entender el sentido de su regulación y los principios éticos a los cuales debe ceñirse el accionar de todos los actores involucrados en el proceso y acceso a la misma. Para ello aquí analizaremos sintéticamente la ley 26.529 de los derechos del paciente, la 25.326 de protección de datos personales, la 26.657 de salud mental, la 25.506 de firma digital, la 27.553 de recetas electrónicas y digitales, la 27675 de Respuesta Integral al HIV y otras ITS, y la Disposición 2/2021 sobre datos sensibles de la Superintendencia de Servicios de Salud.

Derechos del Paciente. Ley 26.529

Esta ley sancionada en el año 2009 y titulada “Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud” consagra en forma expresa los derechos humanos a la

salud, a la confidencialidad, al trato digno, entre otros, de todas las personas que reciban atención sanitaria en nuestro país. Se basa en el principio ético de la Autonomía del Paciente.

Asimismo trae la primera regulación de la Historia Clínica en Argentina, estableciendo su contenido, los sujetos obligados a realizarla, su titularidad y quienes son las personas habilitadas a su acceso. Contiene también un pormenorizado régimen sobre el consentimiento informado como eje central de la autonomía del paciente, todo lo que debe tenerse absolutamente presente a la hora de la implementación de la nueva modalidad electrónica.

Comienza consagrando los derechos del paciente a la vez que enuncia los sujetos pasivos en sentido amplio, al decir que estos derechos son válidos entre el paciente y los profesionales de la salud, el agente del seguro de salud, y cualquier efector de que se trate. Entre los derechos que consagra se encuentra el de Asistencia, por el cual el paciente, sobre todo los niños, niñas y adolescentes, tiene derecho a ser asistido por los profesionales de la salud, sin ningún tipo de discriminación; el derecho al Trato Digno y respetuoso a sus convicciones personales y morales cualquiera sea el padecimiento que presente; derecho a la Intimidad, por el cual toda actividad médico - asistencial cuyo fin sea la obtención, clasificación o utilización de información y documentación clínica del paciente, debe observar el estricto respeto por la dignidad humana, la autonomía de la voluntad, el debido resguardo de la intimidad del mismo y la confidencialidad de sus datos sensibles.

Nos detendremos en el abordaje sobre el derecho a la Confidencialidad, dado que tienen íntima vinculación con el tema que nos ocupa, al respecto la norma en cuestión dice:

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 inc. E, ley 26.529).

Por otro lado, marca un deber ético legal de acatamiento a la autonomía de la voluntad del paciente, basado en el respeto a su dignidad humana y como tal, dueño de su cuerpo, al disponer que el paciente puede aceptar o rechazar las terapias o procedimientos médicos o biológicos, con o sin expresión de causa, y revocar su manifestación de voluntad, como así también tiene derecho a recibir la información sanitaria vinculada a su salud, como por el contrario, negarse a recibirla.

Es plausible que haya normado lo relativo a la Interconsulta Médica, al disponer que el paciente tiene derecho a recibir la información sobre su salud por escrito, a fin de obtener una segunda opinión sobre el diagnóstico, pronóstico o tratamiento relacionados con su estado de salud.

Sobre el marco de la confidencialidad estipula que la información sanitaria sólo podrá ser brindada a terceras personas, con autorización del paciente y en el supuesto de incapacidad o imposibilidad de comprensión, será brindada a su representante legal o, en su defecto, al cónyuge que conviva con el paciente, o la persona que conviva o esté a cargo de la asistencia o cuidado del mismo y los familiares hasta el cuarto grado de consanguinidad. Todo esto cobrará especial importancia cuando nos aboquemos a los sujetos legitimados para el acceso a la información sanitaria contenida en la historia clínica electrónica.

Ahora bien, dijimos que esta ley se centra en el principio de la ética biomédica de Autonomía del Paciente, ahora veremos su principal derivación o sub principio que es el Consentimiento Informado, al que dicha ley lo define como:

Entiéndase por consentimiento informado 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 (…). Art. 5 ley 26.529.

Por lo que, conforme el concepto anterior, el consentimiento informado es comprensible no sólo del diagnóstico presuntivo que emita el profesional tratante, sino de su tratamiento y pronóstico esperable.

Por otro lado, como regla general, el consentimiento será verbal, salvo en los siguientes casos, en los cuales por su gravedad, deberá ser por escrito y suscripto por el paciente: a) Internación; b) Intervención quirúrgica; c) Procedimientos diagnósticos y terapéuticos invasivos; d) Procedimientos que implican riesgos según lo determine la reglamentación de la presente ley; e) Revocación.

A su vez, se establecen excepciones en los cuales si ocurre alguno de estos supuestos, el profesional quedará eximido de requerir el consentimiento informado: a) Cuando mediare grave peligro para la salud pública; b) Cuando mediare una situación de emergencia, con grave peligro para la salud o vida del paciente. Podemos decir entonces, que se tratan de limitaciones al derecho de la autonomía del paciente, el que como todo derecho positivo, es relativo.

El principio de la Autonomía del Paciente recobra mayor vigor cuando la ley establece la posibilidad de la revocación del consentimiento brindado por el paciente, y que el profesional tiene la obligación de acatar, debiendo dejar constancia de ello en la historia clínica. Por otro lado, se encuentra la posibilidad de que el paciente brinde directivas anticipadas sobre su salud, pudiendo

consentir o rechazar determinados tratamientos médicos, lo que debe ser aceptado por el médico, con la limitación de que las mismas no se traten de prácticas eutanásicas.

Finalmente, por aplicación del Principio de Justicia, la norma expresa que ningún profesional interviniente que haya obrado de acuerdo con las disposiciones de la presente ley está sujeto a responsabilidad alguna.

Una vez que hemos analizado todo lo anterior, iremos a otro punto central de esta ley que es la regulación de la Historia Clínica, lo que abordaremos de especial manera, por tratarse del tema que nos ocupa en el presente trabajo.

La ley en su artículo 12 nos brinda el siguiente concepto: "Entiéndase por historia clínica, el documento obligatorio cronológico, foliado y completo en el que conste toda actuación realizada al paciente por profesionales y auxiliares de la salud".

Como tal, debe asentar mínimamente los siguientes registros: La fecha de inicio de su confección: datos identificatorios del paciente, su núcleo familiar; profesional interviniente y su especialidad, Registros claros y precisos de los actos realizados por los profesionales y auxiliares intervinientes, Antecedentes genéticos, fisiológicos y patológicos del paciente, si los hubiere (…), todo acto médico realizado o indicado, sea que se trate de prescripción y suministro de medicamentos, realización de tratamientos, prácticas, estudios principales (..). Los asientos deberán ser realizados sobre la base de nomenclaturas y modelos universales adoptados y actualizados por la OMS.

Recepta la doctrina de la titularidad de la historia clínica en cabeza del paciente, lo que es concordante con el principio de autonomía, y que a su simple requerimiento debe suministrársele copia de la misma, autenticada por autoridad competente de la institución asistencial, colocando un plazo brevísimo de 48hs, salvo casos de urgencia.

Establece que se encuentran legitimados para solicitar la historia clínica: el paciente y su representante legal; el cónyuge o persona en unión convivencial, y los herederos forzosos, en su caso, con la autorización del paciente, salvo que éste se encuentre imposibilitado de darla; Los médicos, y otros profesionales del arte de curar, cuando cuenten con expresa autorización del paciente o de su representante legal. Y brinda una acción judicial urgente que es la acción de "habeas data" en caso de negativa o silencio a brindarle copia de la misma.-

Establece tres características esenciales para la historia clínica que son: integridad, unicidad e inviolabilidad. Por ser íntegra, debe contener 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, con constancia de fecha, firma y sello del profesional actuante.

Por otro lado, 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. Esta Unicidad cobrará otro sentido al establecerse la Historia Clínica Electrónica tal como está regulada por la ley 27.706. Respecto a la inviolabilidad, guarda conexión con las virtudes derivadas del principio de autonomía que son confidencialidad y privacidad, al disponer que la historia clínica es inviolable y los establecimientos asistenciales o profesionales de la salud, en su calidad de titulares de consultorios privados, tienen a su cargo su guarda y custodia, asumiendo el carácter de depositarios de aquélla, por lo que deben instrumentar los medios y recursos necesarios para evitar el acceso no autorizado a la misma.

La ley de los derechos del paciente contiene un artículo clave que permite autorizar desde entonces la historia clínica informatizada, brindando las condiciones para su funcionamiento y algunas pautas de seguridad informática. Así dispone en su artículo 13:

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.

Ley Nacional de respuesta integral al VIH, Hepatitis virales, otras ITS y TBC. Ley 27.675

Esta ley que tiene su basamento en la ley 26.529, consagra de especial forma los derechos derivados del principio de la autonomía del paciente, a favor de una población en situación de vulnerabilidad por el histórico trato discriminatorio que ha recibido socialmente. Por ello es que se les depara una regla de maximización de la confidencialidad con que debe ser manipulada su información sanitaria.

En virtud de ello, establece una serie de características de la prueba diagnóstica de tales enfermedades, la que es voluntaria, gratuita en todos los subsistemas de salud, confidencial y universal. Asimismo que el paciente deberá contar con el debido asesoramiento y participación previa y posterior al testeo.

De forma categórica en su artículo 6° establece como derechos y garantías de los pacientes que padezcan alguna de estas enfermedades, el derecho al resguardo de la confidencialidad, privacidad e intimidad, en acuerdo a la Ley de Protección de los Datos Personales nro. 25.326, y por ello el derecho a no declarar su diagnóstico y/o estadío de su infección.

Como novedad, es la única legislación sobre salud que se dedica a tratar los derechos de las personas privadas de libertad, y otras situaciones especiales como son de aquellos que viven en

hogares convivenciales, o de adultos mayores, y todos aquellos centros de tratamiento de salud mental, de cualquier modalidad de abordaje, al disponer que tienen derecho al trato digno, respetuoso y con las garantías de confidencialidad e intimidad del diagnóstico y tratamiento.

Asimismo se ocupa de otro sector de la población en situación de vulnerabilidad por motivos de edad y de género, al disponer que todo hijo o hija nacido de una mujer y/o persona con capacidad de gestar con VIH, tiene derecho a acceder bajo resguardo de la confidencialidad a prestaciones especiales y gratuitas de leche y tratamiento de inhibición de la lactancia durante los primeros dieciocho (18) meses.

Protección de los Datos sensibles. Disposición 2/2021 de la S.S.S.

En consonancia con la normativa anterior, la Superintendencia de Servicios de Salud de la Nación, emitió la Disposición 2/2021 por la cual declara como datos sensibles aquellos datos personales contenidos en las planillas con el detalle de los beneficiarios con infección por HIV que recibieron prestaciones por parte de los Agentes del Seguro de Salud. Y por lo tanto, se la constituye como información “Reservada y Confidencial”.

Recetas Electrónicas o Digitales. Ley 27553

La presente ley, publicada en el boletín oficial el 27 de julio del 2020, tiene una esencial vinculación con la normativa sobe historia clínica electrónica, y tuvo modificaciones en el último periodo por el DNU 70/23 denominado “Bases para la reconstrucción de la economía argentina”. Dado que establece la obligatoriedad de prescribir los medicamentos en formato electrónico, como así también regula los servicios sanitarios prestados mediante teleasistencia.

Básicamente establece que la prescripción y dispensación de medicamentos, y toda otra prescripción, solo puedan ser redactadas y firmadas a través de plataformas electrónicas habilitadas

a tal fin. Esta ley es de orden público para cualquier profesional de la salud que esté habilitado a prescribir medicamentos y en cualquier ámbito de atención, sea público o privado.

Asimismo permite la utilización de plataformas de teleasistencia en salud, siempre que respeten lo ordenado por la ley de Protección de los Datos Personales y la de Derechos del Paciente.

Pon en cabeza del P.E.N. el deber de normar sobre las plataformas y sistemas electrónicos para tal fin, creando un organismo regulador de las mismas, quien a su vez será el responsable de su fiscalización, debiendo garantizar la custodia de las bases de datos. También será responsable de establecer los criterios de autorización y control de acceso a dichas bases de datos y garantizar el normal funcionamiento y estricto cumplimiento de las leyes vigentes.

Por otro lado, tal como hemos adelantado, la presente norma habilita la modalidad de teleasistencia para el ejercicio de la medicina, odontología y actividades de colaboración de las mismas, e incluye expresamente a los psicólogos, garantizando los derechos del paciente. La teleasistencia solo puede desarrollarse para prácticas autorizadas a tal fin, de acuerdo a protocolos y plataformas aprobadas por la autoridad de aplicación, que es el Ministerio de Salud de la Nación, designado como tal por el decreto reglamentario 98/2023.

Decreto Reglamentario 98/2023 de la ley 27.553

Este interesantísimo decreto reglamentario de las recetas electrónica y digital, como así también de la teleasistencia, trae una serie de innovaciones en cuanto al tratamiento de datos electrónicos, bajo la primacía de los derechos del paciente y todos los sub principios que se desprenden del mismo. El objetivo manifiesto expresamente de esta regulación, es que la prescripción debe estar centrada en la atención integral e integrada de acuerdo a las condiciones del paciente y su historia clínica, garantizando sus derechos a fin de proveer un tratamiento y servicios de calidad.

A fin de poder confeccionar estos documentos electrónicos, crea la Licencia Sanitaria Federal, la que incluye todas las matrículas habilitantes de los profesionales de la salud registrados en la Red Federal, que les otorga una Clave única de identificación del profesional sanitario, que a modo de huella digital, permite identificarlos de forma unívoca, y con ella podrán a los sistemas interoperables del Sistema Sanitario Argentino.

En el artículo 1 de su anexo, define receta electrónica a la que la diferencia de la receta digital, según la rúbrica del profesional haya sido realizada con firma electrónica o firma digital conforme la normativa que la regula.

A su vez establece como requisitos de carácter obligatorio para estas recetas: 1) Identificación mediante la clave de identificación supra mencionada. 2) Contenido conforme lo indicado legalmente 3) Vigencia de la receta. 4) Integridad e inalterabilidad, salvo que se trate de modificaciones controladas vinculadas a los procesos necesarios para las anotaciones. 5) seguridad, disponibilidad, inviolabilidad y protección de datos personales, conforme la normativa vigente. 6) Interoperabilidad, mediante la cual la receta digital o electrónica utilizará estándares sintácticos y semánticos que permitan el intercambio y el uso de la información con fines sanitarios, estadísticos, de fiscalización y epidemiológicos, a través de la Red Nacional de Interoperabilidad en Salud.

Por otro lado, define el concepto de Teleasistencia y ordena que las plataformas utilizadas en tal sentido, deben estar previamente inscriptas y aprobadas por el Ministerio de Salud:

Debe entenderse por Teleasistencia a la provisión de servicios de salud a distancia mediante la utilización de tecnologías de la información y comunicaciones de forma sincrónica o asincrónica, realizada dentro del territorio nacional, por el equipo de salud, para la promoción, prevención, diagnóstico, tratamiento y rehabilitación, conforme demás requisitos que disponga cada autoridad sanitaria y la normativa vigente. (Art. 1 inc. B)

Establece en cabeza del Ministerio de Salud como autoridad de aplicación de la presente ley que debe regular una política de seguridad de la información y protección de datos personales, que deben cumplir sistemas informáticos de teleasistencia, prescripción y dispensa de receta electrónica o digital.

Asimismo establece una serie de responsabilidades legales y de seguridad informática, que son novedosos y totalmente necesarios a fin de salvaguardar los derechos de los pacientes en los ámbitos digitales, al ordenar que los servicios plataformas que utilicen para las recetas o para la teleasistencia deben constituirse como empresas responsables en el territorio argentino, del tratamiento de datos, obligándose a hacerlo de manera confidencial, resguardar las credenciales y accesos para garantizar la seguridad, privacidad, finalidad, oportunidad, veracidad e inviolabilidad de los datos.

El decreto establece todo ello con la finalidad de evitar el uso no autorizado de la información sanitaria, lo que en la práctica se conoce como fuga de datos, al disponer que: “Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado” (Inc. E).

Lo que más nos interesa, por su íntima relación con el tema central de este trabajo, es que la reglamentación elige las medidas de seguridad informática que ha considerado mejores y a su vez introduce el tema del uso de la inteligencia artificial en el campo de la salud. Categóricamente ordena que deben disponer de tecnología con los estándares para sistemas de información en salud determinados por la autoridad regulatoria y que en caso de uso de tecnologías con transmisión de audio y video en simultáneo, se deben utilizar sistemas con cifrado y encriptado, vigentes y actualizados que aseguren los estándares de mayor seguridad. En cuanto al uso de inteligencia artificial, ordena que se observen las restricciones y limitaciones que se les imponga, quedando

dicho uso sólo de apoyo a la toma de decisiones profesionales, siempre la supervisión de profesionales de la salud.

Finalmente establece una diferenciación en el uso de datos sanitarios, a fines de liberar de responsabilidad a aquellos profesionales que deban utilizarlos para investigaciones científicas o con fines estadísticos, epidemiológicos o de políticas sanitarias, al disponer que el dato sanitario disociado no se considerará dato sensible y podrá ser utilizado con dichos fines.

Firma Digital. Ley 25.506

La importancia del estudio de la presente ley para nuestro trabajo, radica en que reconoce el empleo de la firma electrónica y de la firma digital en los documentos digitales, otorgándole eficacia jurídica en las condiciones que establece, igualándolo al documento escrito. Entonces gracias a la firma digital, es posible otorgar validez a la historia clínica electrónica.

Con meridiana claridad lo expresa el Dr. Vitolo, F. La ley modifica sustancialmente el concepto de documento contenido en el Código Civil, asociado a la forma escrita, (art. 978 CC) y realizado en soporte de papel, equiparando a la firma ológrafa con la firma digital y la firma electrónica. Antes de la ley mencionada, cualquier documentación digital no tenía el carácter de documento que ahora sí tiene. Ley vigente 25.506 de Firma Digital es el instrumento jurídico que hace posible que las historias computarizadas no sean cuestionables desde el punto de vista legal. (Vitolo, 2009).

En su artículo 2 la norma define el concepto y condiciones de existencia de la firma digital:

Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar

cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

También define el concepto de firma electrónica, cuya diferencia radica en que el medio de identificación carece de alguno de los requisitos legales para ser considerada firma digital y por ello no goza de la presunción de autoría e integridad, como ya veremos enseguida.

Por otro lado define en qué consiste un documento digital en su artículo 6: “Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura”. Lo que es de importancia porque es el sustento de los asientos electrónicos que constituyen la HCE.

Ahora bien, lo fundamental de la firma digital, es que la misma goza de presunciones iuris tantum que logran que sea satisfactoria a los fines legales, estos son: presunción de autoría del remitente, de que la firma digital pertenece al titular del certificado digital y presunción de integridad, de que el documento digital no ha sido modificado luego de su firma.

A su vez establece serios requisitos para que la firma digital sea válida: la misma debe haber sido creada durante el período de vigencia del certificado digital, ser debidamente verificada según el procedimiento de verificación correspondiente y que dicho certificado haya sido emitido o reconocido por un certificador licenciado. Siendo válida, otorga carácter de originales a los documentos electrónicos firmados digitalmente y los reproducidos en formato digital, y como consecuencia de ello, poseen valor probatorio como tales.

Finalmente la obligación de conservarlos se considera cumplida siempre que sea según los procedimientos que determine la reglamentación, y que sean accesibles para su posterior consulta,

permitiendo determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

Protección de Datos Personales. Ley 25.326

Veremos esta ley sancionada en el año 2000, por su esencial importancia para el tratamiento de los datos personales del paciente, incorporados en la historia clínica. Por cuanto contiene principios generales relativos a la protección de datos, asimismo los derechos de los titulares de datos, sanciones y control para los usuarios y responsables de registros y la acción judicial de protección de los datos personales.

El objeto de esta ley es proteger de forma integral 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 (art. 1).

Define en su artículo 2 a los datos sensibles, que son aquellos “Datos personales que revelan (…) información referente a la salud o a la vida sexual”. Y establece que el titular de los datos es la persona cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

Ordena que las bases de datos deban estar debidamente inscriptas, observando los principios y obligaciones que establece la ley, como así también regula la calidad de los datos que se almacenen, los que deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los mismos no pueden recolectarse por medios ilegales o desleales, tampoco pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Los datos deben ser exactos y actualizarse en caso necesario. (art.4).

Es el responsable del archivo el obligado a suprimir o sustituir los datos total o parcialmente inexactos, o que sean incompletos, sin perjuicio de los derechos del titular.

La ley regula de forma pormenorizada el tratamiento de los datos personales, con un enfoque centrado en la persona, dado que exige el consentimiento para el tratamiento de los datos relativos a la salud personal, el que debe constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias, salvo determinadas excepciones que establece.

Asimismo en su artículo 6 ordena que se debe informar a los titulares de los datos, la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios; asimismo la existencia del banco de datos, y la identidad de su responsable; el carácter obligatorio o facultativo de las respuestas, las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos, la posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos.

Finalmente se establece que ninguna persona puede ser obligada a proporcionar datos sensibles, pero sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley o con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Por otro lado, dispone las obligaciones para los establecimientos sanitarios y los profesionales que pueden recolectar y tratar los datos de los pacientes que acudan a los mismos, respetando los principios del secreto profesional. Asimismo que deben 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. Tienen prohibido registrar datos

personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad (arts. 8, 9, 10).

En el capítulo III la norma establece los derechos de los titulares de los datos, que por una cuestión de síntesis, nos remitiremos a lo que vamos a explicar en el apartado de Historia Clínica Electrónica, por cuanto guarda similitud en su tratamiento: derecho de información, derecho de acceso, contenido claro y accesible de la información.

En cuanto al derecho de rectificación, actualización o supresión, ordena que toda persona tiene derecho, de forma gratuita, a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad. Y el responsable o usuario del banco de datos, cuenta con un plazo máximo de cinco días hábiles para solucionarlo, bajo apercibimiento de promover inmediatamente a la acción de habeas data regulada en el Capítulo VII de la norma.

Historia Clínica Electrónica

Hemos llegado al punto central de nuestro trabajo, que es la flamante regulación de la historia clínica electrónica en Argentina, mediante la ley nro. 27.706 publicada en el Boletín Oficial el 16 de marzo de 2023, denominada Programa Federal Único de Informatización y Digitalización de Historias Clínicas de la República Argentina, y reglamentada mediante el Decreto nro. 393/2023 que ha entrado en vigencia a partir de su publicación en el Boletín Oficial, en fecha 31 de julio del mismo año, por lo que se encuentra rigiendo actualmente en nuestro país.

La norma crea el Programa Federal Único de Informatización y Digitalización de las Historias Clínicas de todo el país, con la finalidad de instaurar progresivamente, el Sistema Único de Registro de Historias Clínicas Electrónicas, respetando el marco normativo que hemos reseñado en el presente trabajo.

El Poder Ejecutivo ha elegido como autoridad nacional de aplicación al Ministerio de Salud, y de las funciones que le otorga, consideramos primordial la de determinar las características técnicas y operativas de la informatización y digitalización de las historias clínicas; y por otro lado, la de elaborar un protocolo de carga de las mismas, así como diseñar e implementar un software coordinando la implementación interjurisdiccional. También debe generar un marco de interoperabilidad entre los sistemas que se encuentren en funcionamiento con los sistemas a crear, tanto en el sector público, privado y del ámbito de la seguridad social; e instalar el software de forma gratuita en todos los hospitales públicos o privados.

Asimismo dispone la creación de una Comisión Interdisciplinaria de expertos a los efectos de coordinar con las autoridades en el marco del Consejo Federal de Salud (COFESA), la implementación de la presente ley en cada una de las jurisdicciones.

Concepto y Características

El artículo 1 del reglamento nos trae el concepto de Historia Clínica Electrónica (HCE), a la vez que define sus características esenciales, las que operan como garantía de su seguridad jurídica y establece el marco normativo aplicable:

Conjunto de documentos digitales y/o electrónicos, en el que se registra toda actuación realizada por profesionales y auxiliares de la salud, todos los procesos asistenciales indicados y recibidos por el o la paciente, aceptados o rechazados y los datos actualizados de su estado de salud, para garantizar una asistencia adecuada. La HISTORIA CLÍNICA ELECTRÓNICA (HCE) es integral, auténtica, inalterable, perdurable, única, inviolable y recuperable en tiempo y forma, respecto de los datos contenidos en ella, de conformidad a lo establecido en las Leyes N° 25.326 y su modificatoria, N° 25.506 y N° 26.529 y sus respectivas modificatorias.

Contenido

La ley en su art. 8 tercer párrafo, establece que forman parte de la HCE los consentimientos informados, las hojas de indicaciones médicas y/o profesionales, las planillas de enfermería, los protocolos quirúrgicos, las prescripciones dietarias, certificados de vacunación, los estudios y prácticas realizadas, rechazadas o abandonadas.

A su vez establece que en el Sistema Único de Registro de HCE se deja constancia de toda intervención médico-sanitaria a cargo de profesionales y auxiliares de la salud, de cualquier jurisdicción y tanto de establecimientos privados como públicos y de la seguridad social.

Por otro lado es obligatorio que este Sistema cuente los datos clínicos de la persona o paciente, de forma clara y de fácil entendimiento, desde el nacimiento hasta su fallecimiento. No pudiendo ser alterada, sin que quede registrada la modificación pertinente, aun en el caso de que tuviera por objeto subsanar un error acorde a la ley de habeas data.

Titularidad

La presente ley recepta la teoría de que la historia clínica es propiedad del paciente, dado que la información sanitaria que consta en la misma, se trata sobre su propia salud y ha sido cedida por él mismo al profesional de la salud, mediante la confianza depositada para su tratamiento, aguardando que la utilice con determinados fines terapéuticos y respetando su derecho a la confidencialidad. Es así que en su artículo 8, la ley expresa:

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.

Asimismo establece que en caso de incapacidad del paciente o imposibilidad de comprender la información a causa de su estado físico o psíquico, la misma debe ser brindada a su representante legal o derecho habientes.

Cuestión diferente es el tema de quien es el depositario o custodio de la misma, por lo que el decreto reglamentario, en los articulo 1 y 3 de su anexo, se encarga de establecerlo en cabeza de los establecimientos asistenciales públicos o privados y los o las profesionales de la salud, en su calidad de titulares de consultorios privados, quienes a su vez deben instrumentar los para evitar el acceso a la información por personas no autorizadas.

Visto lo anterior y aunque parezca una obviedad para muchos, no debe confundirse titularidad de la HCE con custodia de la misma. Valga la aclaración para quienes consideran que se debe exigir algún procedimiento legal como una orden judicial para que el paciente pueda acceder a su historia clínica, lo que como ya hemos visto en el análisis efectuado en todo este trabajo, es algo erróneo, puesto que siendo el paciente el titular de la misma, tiene el derecho de acceder a su simple petición.

Accesibilidad

Hemos visto la importancia de la historia clínica para el paciente, por cuanto este registro contiene información sanitaria que hace a la correcta atención de su salud en todos los niveles y especialidades. Con este objetivo es que la ley en su artículo 7 garantiza que tanto los pacientes como los profesionales de la salud y personas autorizadas, puedan acceder al Sistema Único de Registro de HCE desde cualquier lugar del territorio nacional, para lo cual la información debe estar disponible en todo momento y en todos los establecimientos asistenciales y en este punto debemos destacar que la reglamentación, en sus artículos 1 y 5, establece diferentes accesos de seguridad en pos de asegurar el derecho a la confidencialidad, lo que estudiamos con especial interés en atención

a que es uno de los principales objetivos de las recomendaciones de Ética y Gobernanza en materia de inteligencia artificial, que ha publicado hace dos meses la OMS.

La reglamentación dispone que es el Ministerio de Salud, en su carácter de organismo de aplicación, quien establece los estándares que define los perfiles de acceso a este sistema y para ello debe adoptar el uso de accesos restringidos o cualquier otra técnica idónea para asegurar su integridad. La ley en su artículo dispone que existen por lo menos tres (3) niveles de acceso: unos tendrán acceso solo a la consulta, otros además podrán actualizar la información y los que tengan mayor control podrán también hasta modificarla. Finalmente se dispone que el sistema garantizará la trazabilidad, la que es definida del siguiente modo: "Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información y/o sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad, dejando rastro del respectivo acceso". (Art. 7 inc. 1 b, op. cit.).

Todo ello condice con la Declaración de Lisboa sobre los Derechos del Paciente, que en su Principio 7 consagra el Derecho al acceso a la información del paciente, al disponer que:

(a) El paciente tiene derecho a recibir información sobre su persona registrada en su historial médico y a estar totalmente informado sobre su salud, inclusive los aspectos médicos de su condición. Sin embargo, la información confidencial contenida en el historial del paciente sobre una tercera persona, no debe ser entregada a éste sin el consentimiento de dicha persona. (…).

(c) La información se debe entregar de manera apropiada a la cultura local y de tal forma que el paciente pueda entenderla. (…).

Sistema Informático de HCE

Lo novedosos de esta ley es que no se limita a regular la creación de documentos digitales sanitarios como las historias clínicas electrónicas, sino que además dispone la creación de un

software denominado “Sistema de Historias Clínicas Electrónicas”, al que desde ahora en más, nos referiremos a él simplemente como el sistema.

El anexo del decreto reglamentario en su artículo 1, dispone que este sistema de información debe contar con autonomía tecnológica suficiente para soportar su funcionamiento y asegurar su correcto uso, debiendo estar inscripto en el Registro de Dominios de Interoperabilidad en Salud, que también se crea.

El Ministerio de Salud en cuanto Autoridad de Aplicación tiene varias funciones dispuestas por la reglamentación, de las cuales consideramos como elementales las de promover el diseño y la implementación interjurisdiccional del software de Historia de Salud Integrada, colocándolo a disposición de todas las jurisdicciones del país, y debe ser de uso gratuito, sobre la base de un programa de código abierto, que puede ser accedido, utilizado y modificado, libre y gratuitamente por cada dominio, en los términos establecidos por la mencionada Resolución.

También establece que este sistema debe contar con un marco de interoperabilidad, entre los sistemas que ya están funcionando (por ejemplo el del Hospital Italiano, el de la provincia de San Luis, etc.), con los que vayan a crearse tras esta ley, asimismo tanto del sector público como del privado. Ello con el fin de crear la Red Nacional de Interoperabilidad en Salud, a fin de facilitar la integración de todos estos sistemas de salud.

Establece una serie de requisitos que hacen a la seguridad informática, como es la obligatoriedad de la autenticación de las personas que intervengan en los sistemas, para lo cual deberán articular con los organismos públicos a fin de cruzar los datos, por ejemplo el Registro Nacional de las Personas, los Colegios Profesionales, la Superintendencia de Servicios de Salud, etc. La autenticación será posible gracias a la utilización de la Licencia Sanitaria Federal, creada por el decreto 98/2023 que toma como base de datos las matrículas vigentes en la “Red Federal de

Registros de Profesionales de la Salud" (REFEPS). La norma reiterativa la norma en cuanto este Sistema debe adecuarse a lo establecido por las leyes aquí estudiadas.

En el artículo 6 y en la última parte del artículo 8, vuelve a ordenar el carácter confidencial de los datos volcados en el Sistema, especificando que el Ministerio de Salud establece los responsables de la administración y el resguardo de la información clínica; asimismo que cualquier acción referida a la información debe efectuarse en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad, acceso y trazabilidad, garantizándose la autenticación de las personas que intervengan en el Sistema, el libre acceso y seguimiento por parte del paciente, la recuperación de archivos y la perdurabilidad de la información, la posibilidad de auditoría.

A modo de corolario establece que "La información constituye documentación auténtica y, como tal, es válida y admisible como medio probatorio, haciendo plena fe a todos los efectos, siempre que se encuentre autenticada". (Art. 6 inc. G, op. cit.)

Modelo Bioético de Autonomía del Paciente

Habiendo analizado la legislación especial sobre la materia que nos ocupa, ahora nos vamos a ocupar de estudiar los principios bioéticos contenidos en las normas, sobre todo el de autonomía del paciente y su derivado de confidencialidad en el tratamiento de sus datos personales. Para posteriormente poder analizar el flamante documento de la Organización Mundial de la Salud (OMS), sobre Ética y Gobernanza de la Inteligencia Artificial para la salud, que ha sido publicado hace poco más de dos meses.

Principio de autonomía en la Constitución Nacional y el Código Civil:

En este punto compartimos el análisis que realiza Basterra, Marcela, quien sostiene:

El principio de autonomía personal que también podemos denominar de reserva o autoreferencia, está contenido en el artículo 19 de la Ley Fundamental (…) Este principio implica que cada persona adulta, mayor de edad –excluye a los menores– con consentimiento, es decir, que posea discernimiento, intención y libertad –no se aplica a los incapaces que no comprenden sus actos–, puede escoger el que considere "mejor plan de vida" para sí misma, aunque éste implique un daño personal. Sólo el daño a terceros opera como límite a la elección del propio plan elegido. (…) Este criterio ha sido elaborado por la Corte Suprema en el precedente Bahamondez y ratificado en el fallo Albarracini. (Basterra).

La autonomía del paciente se trata de un derecho humano personalísimo y como tal pertenece a todo ser humano y es vitalicio e irrenunciable. Siguiendo la línea constitucional, nuestro actual Código Civil y Comercial de la Nación en su art. 59, regula el concepto y requisitos del consentimiento informado, que guarda similitud con lo normado por el artículo 5 de la ley 26.529:

El consentimiento informado para actos médicos e investigaciones en salud 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 (…). Nadie puede ser sometido a exámenes o tratamientos clínicos o quirúrgicos sin su consentimiento libre e informado, excepto disposición legal en contrario (…).

Entonces vemos que se torna imprescindible también el tomar en consideración las necesidades del paciente, sus convicciones religiosas y morales, acorde a los precedentes judiciales reseñados, dado el modelo centrado en la persona, que ha sido acatado por nuestra legislación. El

paciente deposita su confianza en el profesional que lo atiende, a fin de tratar de conseguir certeza sobre su estado de salud y un necesario tratamiento en caso necesario.

Tal como enseña Fliguer, J. en su clase de Filosofía Práctica: “La autonomía considera los valores y creencias del paciente como el principal determinante de la responsabilidad moral del médico. Como virtudes derivadas del principio de autonomía, encontramos la Veracidad, Confidencialidad, Privacidad., Fidelidad, de allí la necesidad de que el consentimiento que se preste sea informado”.

Confidencialidad y Privacidad

Ahora bien, es importante que toda la información sobre el estado de salud del paciente, ya sea su diagnóstico, tratamiento o de cualquier otro tipo por el cual se lo pueda identificar, se deba manejar con estricta confidencialidad incluso después de su muerte. Nos hacemos eco de lo que célebres profesionales de la salud manifiestan al respecto:

Hablando en términos de bioética, podemos ver principalmente dos principios comprometidos en lo referente a la preservación del secreto: la autonomía y la no maleficencia. El paciente que acude a un centro sanitario establece una relación quid pro quo en la que deberá ceder información a cambio de una adecuada atención (…) Es solo el propio interesado quien puede decidir qué información pertenece a su más estricta intimidad, según sus propios criterios. Existe además un deber moral de fidelidad para con el paciente. Se deben respetar los acuerdos a que se llegan (pacta sunt servanda), y esto incluye el acuerdo implícito acerca de la confidencialidad de la información que se maneja en la actuación sanitaria. (J. Antomás, S. Huarte del Barrio).

La confidencialidad es una derivación del principio de autonomía del paciente y debe entenderse como un derecho del mismo y una obligación de los profesionales de la salud. Tal es así

que la Asociación Médica Mundial en la Declaración de Lisboa Sobre los derechos del Paciente, expresó sobre el derecho al secreto:

(…) Excepcionalmente, los descendientes pueden tener derecho al acceso de la información que los prevenga de los riesgos de salud. La información confidencial sólo se puede dar a conocer si el paciente da su consentimiento explícito o si la ley prevé expresamente eso. Se puede entregar información a otro personal de salud que presta atención, sólo en base estrictamente de "necesidad de conocer", a menos que el paciente dé un consentimiento explícito. Toda información identificable del paciente debe ser protegida. La protección de la información debe ser apropiada a la manera del almacenamiento.

En consonancia, el Código de Ética de la Asociación Médica Argentina, consagra de modo especial la confidencialidad al tratar sobre la historia clínica electrónica, mediante el art. 185 que dispone: “En caso de computarización de la Historia Clínica deberán implementarse sistemas de seguridad suficientes para asegurar la inalterabilidad de los datos y evitar el accionar de violadores de información reservada.”

Asimismo establece ciertos requisitos inexorables como son la inviolabilidad, autoría, confidencialidad, secuencialidad, temporalidad (time stamping), disponibilidad, integridad, durabilidad e inalterabilidad de la información, integridad impidiendo la adulteración, transportabilidad e Impresión.

Al respecto, veremos ahora lo que dicho Código ordena sobre los requisitos que tienen íntima vinculación con el objeto de este trabajo. Sobre la inviolabilidad dispone que “la información no pueda ser adulterada. Una vez ingresados los datos no pueden modificarse. Cualquier corrección automáticamente se agrega al final del texto preservando la cita original. Se debe impedir el ingreso no autorizado de datos en el sistema de información (…)”.

Asimismo sobre la autoría, ordena que el sistema deberá otorgar garantías acerca de la identidad de quien ingresa los datos (…) y en cuanto a la confidencialidad, se debe impedir que los datos sean leídos, copiados o retirados por personas no autorizadas. (…) y que no todos pueden tener acceso a toda la información. Para ello se utilizan técnicas de encriptación. (Asociación Médica Argentina, 2001).

Orientaciones de la OMS Sobre la Ética y la Gobernanza de la Inteligencia Artificial ante la Problemática Vigente.

Este importante documento llamado *"Ethics and governance of artificial intelligence for health Guidance on large multi-modal models"* (Ética y gobernanza de Inteligencia artificial para la salud - Orientación sobre grandes modelos multimodales) publicado en inglés por la Organización Mundial de la Salud (OMS) el 18 de enero del corriente año. Brinda más de 40 recomendaciones para la consideración de los gobiernos, los proveedores de atención de salud y las empresas de tecnología en materia de salud, para que puedan garantizar el correcto uso de los grandes modelos multimodales y de inteligencia artificial en la promoción y protección de la salud de las personas.

El documento ha sido elaborado por un comité de expertos, basándose en el publicado tres años atrás por dicha organización y consta de varias secciones, de las cuales las que más nos interesa para el presente trabajo son la sección 4 que resume las políticas públicas, las leyes y los principios éticos que podrían aplicarse a la utilización de la inteligencia artificial (IA) en el ámbito de la salud, la sección 5 que describe los principios éticos fundamentales y finalmente la sección 6 que aborda los problemas éticos que han sido identificados por el grupo de expertos y que puede intentarse una solución mediante esos principios rectores.

La OMS aquí nos enseña que "Un principio ético es una declaración de un deber o una responsabilidad en el contexto del desarrollo, implementación y evaluación continua de tecnologías

de IA para la salud" (P. 23 op. cit.). A continuación describe aquellos principios que se basan en requisitos éticos básicos que se aplican a todas las personas y se consideran no controvertidos:

1) Evitar dañar a otros (a veces llamado "no hacer daño" o no maleficencia).

2) Promover el bienestar de los demás cuando sea posible (a veces llamado "beneficencia"). Los riesgos de daño deben minimizarse y al mismo tiempo maximizar los beneficios.

3) Garantizar que todas las personas reciban un trato justo, lo que incluye el requisito de garantizar que ninguna persona o grupo sea objeto de discriminación, abandono, manipulación, dominación o abuso (a veces llamado "justicia" o "imparcialidad").

4) Tratar con las personas de manera que respeten sus intereses al tomar decisiones sobre su vida y su persona, incluidas las decisiones sanitarias (a veces llamado "respeto a las personas" o "autonomía"). Se pueden derivar requisitos morales adicionales, por ejemplo, salvaguardar y proteger la privacidad individual (…) que es importante para permitir que las personas puedan controlar información sensible sobre sí mismas; la autodeterminación (respeto a su autonomía) y evitar daños. (P. 23 op. cit.).

Estos principios éticos buscan orientar, a modo de brújula, a los gobiernos y a todas las demás partes interesadas en la toma de decisiones en la implementación, desarrollo y evaluación de la IA en el campo de la salud, a fin de que no pongan en riesgo los derechos del paciente aquí reseñados ni tampoco choquen contra cuestiones de importancia moral.

La OMS enfatiza, en la página 48 del texto citado, en que todos los sistemas o herramientas de IA utilizados en la atención sanitaria deben respetar los principios bioéticos y los derechos humanos relativos a la dignidad, la autonomía o la privacidad de una persona.

Asimismo que el hecho de que un algoritmo de IA se considere de "bajo riesgo" no lo exime del escrutinio, y un desarrollador o proveedor debe asegurarse de que el algoritmo respete los

derechos humanos y las obligaciones éticas, debiendo evaluarse su impacto a fin de analizar si es posible su aplicación de forma segura.

Visto lo anterior, ahora lo OMS nos indica los posibles riesgos que deben abordarse al implementar un servicio de atención médica, utilizando un modelo de lenguaje multimodal (LMM) o inteligencia artificial:

Los riesgos durante la implementación pueden deberse a la imprevisibilidad de los LMM y las respuestas que proporcionan, a la posibilidad de utilizar un modelo de base de propósito general de una manera que no fue anticipada ni por el desarrollador ni por el proveedor, y porque las respuestas generadas por un LMM pueden cambiar con el tiempo. Los principales riesgos que deben abordarse al implementar un LMM son: respuestas inexactas o falsas, sesgo, privacidad de los datos ingresados y publicados por un LMM, accesibilidad y asequibilidad de un LMM, impactos en el trabajo y el empleo, sesgo de automatización y degradación de habilidades entre la calidad de las interacciones entre los proveedores de atención médica y los pacientes. (P. 53 op. cit.).

Asimismo en el sumario ejecutivo los presenta en la Tabla 2. De los cuales pasaremos a explicar los más relevantes para el presente trabajo, que son la sobreestimación de los beneficios de la inteligencia artificial, por la cual puede haber una tendencia al "solucionismo tecnológico", mientras se ignoran o minimizan los desafíos en su uso, incluyendo su seguridad, eficacia y utilidad. Por otro lado que debido a la brecha digital, puede erosionarse la accesibilidad y asequibilidad de estos sistemas.

Otro de los riesgos que advierte, es que la documentación recopilada mediante tecnología de IA, pueda utilizarse para codificar sesgos en detrimento de grupos identificables, especialmente si ya están marginados, siendo esto una amenaza para la inclusividad y la equidad, ya que puede dar lugar a una desviación, a menudo arbitraria, en la igualdad de trato (…) y por ello es que solicita que

ninguna tecnología, sea de IA o de otro tipo, apoye o empeore las formas existentes de sesgo y discriminación.

Además, la falta de preservación y protección de la privacidad y la confidencialidad podría socavar la confianza en los sistemas de salud por parte de los pacientes.

Hay grandes riesgos de ciberseguridad, mediante los ataques maliciosos o la piratería informática que atentan contra la seguridad y la confianza en el uso de los LMM en la atención médica. El documento lo explica de una manera contundente, al advertir que:

A medida que los sistemas de atención médica se vuelven cada vez más dependientes de la IA, las tecnologías podrían ser objeto de ataques maliciosos y piratería informática y algunos sistemas podrían cerrarse, con la manipulación de los datos utilizados para entrenar el algoritmo, cambiando así su rendimiento y recomendaciones, o los datos podrían ser "secuestrados" para pedir un rescate. (P. 22 op. cit.).

Otro riesgo de seguridad particular es la introducción de datos confidenciales en las LMM que no están protegidas contra la divulgación o el uso no autorizados. Actualmente se produce lo que se denomina “inyección rápida” para lo cual no hay solución conocida y consiste en un ataque donde un tercero introduce datos en los sistemas a fin de que se comporte de una manera no prevista por el desarrollador del software.

Ante todos estos riesgos esperables, la OMS solicita que los ministerios de salud y las universidades capaciten a los profesionales de la salud a fin de identificar y comprender las preocupaciones sobre el uso apropiado de la inteligencia artificial, el evitar el sesgo de automatización y conocer los riesgos de ciberseguridad. Asimismo también es necesario involucrar y educar a los pacientes en tal sentido.

Por otro lado advierte que “la existencia de un marco de derechos humanos no elimina la necesidad de deliberación ética continua. De hecho, gran parte de la ética pretende ampliar y complementar las normas y obligaciones establecidas en los acuerdos de derechos humanos”. (P. 41).

Solicita que de modo especial se proteja la autonomía del paciente, que implica los deberes relacionados de proteger la privacidad y confidencialidad y garantizar el consentimiento informado y válido mediante la adopción de medidas legales apropiadas. Estas deben ser plenamente apoyadas y aplicadas por gobiernos y respetado por las empresas y sus diseñadores de sistemas, programadores, creadores de bases de datos y otros. Asimismo que cuando se empleen algoritmos de aprendizaje automático en el diagnóstico, pronóstico y planes de tratamiento, se debe informar al paciente e incorporarse en su consentimiento informado.

Al respecto es interesante estudiar lo declarado en la introducción a este documento: La Declaración Universal de Derechos Humanos, que incluye pilares de los derechos de los pacientes como dignidad, privacidad, confidencialidad y consentimiento informado, podrían redefinirse drásticamente o ser socavados a medida que las tecnologías digitales se afianzan y se expanden. El rendimiento de la IA depende (entre otros factores) de la naturaleza, el tipo y el volumen de datos e información y las condiciones bajo las cuales dichos datos fueron recopilados. La búsqueda de los datos, ya sean del gobierno o de las empresas, podrían socavar la privacidad y la autonomía, al servicio de la vigilancia gubernamental o privada o del beneficio comercial. Si la privacidad y la autonomía no están aseguradas, la consiguiente limitación de la capacidad de ejercer plenamente la gama de derechos humanos (…) y derechos sociales y económicos (como el acceso a la atención sanitaria y educación), podrían tener un impacto más amplio. (P. 26).

Asimismo cobra especial relevancia el capítulo 6 titulado “Desafíos éticos del uso de

inteligencia artificial para el cuidado de la salud", donde estudia los riesgos sobre la recopilación y uso de datos, manifestando que es preocupante que la comercialización de datos pueda incluir la pérdida del control sobre los datos sin ningún tipo de consentimiento para dicho uso secundario y de ese modo perderse el derecho a la autonomía del paciente. Es decir, que estos datos o los generados por ellos, puedan ser utilizados por la empresa o un tercero, en detrimento de la privacidad del paciente, ya sea de forma intencional o por una violación de seguridad.

Los datos sanitarios de los pacientes son datos sensibles, que una vez expuestos, es muy difícil que pueda lograrse la restauración de su derecho a la privacidad, de allí la importancia de promover controles de seguridad informática y autenticación para el acceso y manipulación de los mismos.

Conclusión.

Hemos llegado al final de este trabajo, donde analizamos el marco normativo preexistente a la ley de Historia Clínica Electrónica, conjuntamente con su regulación, con la finalidad de entender los derechos del paciente que se encuentran involucrados. Dado que si bien no desconocemos los múltiples beneficios que trae la tecnología en materia de e-salud y la inteligencia artificial, es dable destacar que también debemos hablar de los riesgos de una incorrecta aplicación de la misma, que pueda conculcar la confidencialidad y dignidad con que deben ser tratados los pacientes y su información sanitaria. Por ello es que nos parece importante el estudio realizado por expertos de diferentes países y que ha sido volcado en el flamante documento de la ONU que aquí hemos visto, en el que realiza una serie pormenorizada de recomendaciones para el tratamiento de la inteligencia artificial aplicada a la salud humana.

Podríamos observar por ejemplo cómo ha sido la práctica de la Historia Clínica Electrónica en países de avanzada como España, Bélgica y Australia, pero eso será objeto de un

posterior trabajo, porque en estos momentos en que aún no se está desarrollando, nos parece precipitado extrapolar experiencias que no sabremos si serán de una posible aplicación. Por ello en este actual estudio hemos preferido realizar un análisis conforme al estado actual del arte en Argentina.

Los beneficios de la inteligencia artificial para el tratamiento de la salud, son evidentes, pues permite incorporar protocolos de estudio y tratamiento, asimismo vademécum institucionales que permitirían evitar contraindicaciones medicamentosas, etc. Pero necesitamos hablar de los riesgos, ya que se encuentra en juego los principios éticos de la autonomía del paciente, específicamente lo vinculado a su privacidad y a su consentimiento informado.

Por lo que será importante capacitar a los profesionales de la salud y a todos los demás actores que intervengan en el acceso de la información sanitaria del paciente, no solamente en cuanto al marco legal al que deben sujetarse, principalmente en la ley de protección de datos personales y específicamente los datos sensibles como son los que se vuelcan a la historia clínica, sino que también deberán tener una formación en materia de seguridad informática, a fin de evitar los riesgos reseñados por la OMS como son la divulgación no autorizada de datos personales, los ciber-ataques, los sesgos de información, la falta de accesibilidad por la brecha digital existente en nuestro país, etc.

Nótese por ejemplo, las grandes dificultades que atravesaron miles de pacientes en nuestro país cuando se implementó el Certificado Médico Oficial (CMO) como requisito obligatorio para que las personas con discapacidad puedan acceder a una pensión no contributiva por invalidez. Dado que la mayoría de los centros de salud de gestión pública no contaban con algo indispensable como es conectividad a internet, ni mucho menos los profesionales de la salud estaban capacitados para manejar el software que permitía cargar dicha información en ANSES, todo lo cual redundó en que muchos no puedan acceder a dicho trámite.

Algo similar ocurrió con la pandemia COVID19 cuando se comenzaron a realizar las primeras recetas digitales en PAMI, con todos los inconvenientes suscitados por las mismas razones o por la ausencia de firma digital en los términos que ordena la ley. Los resabios que dejaron estas experiencias para los afiliados en mayor grado de vulnerabilidad, como son los adultos mayores y las personas con discapacidad, por las brechas digitales existentes en organismos públicos, nos dan muestra de este principal riesgo, al que por supuesto puede sumarse los demás, por cuanto es el inicial.

Estamos en condiciones de decir que la brecha digital en nuestro país, es un grave riesgo para la equidad en materia tecnológica aplicable a la salud.

Pero lo que más nos preocupa es la falta de capacitación sobre mecanismos mínimos de seguridad que eviten las fugas de información o los ciberataques a la información confidencial de los pacientes.

Nos parece sumamente importante para evitar las malas prácticas en materia de manipulación de los registros informáticos, que se solicite a las entidades representativas de los responsables de bases de datos, que elaboren los códigos de ética para su tratamiento, conforme lo ordena el art. 30 de la ley 25.326. Asimismo que se capacite a todos los actores que puedan tener acceso a la historia clínica electrónica, en materia de sanciones administrativas y penales, como las establecidas en dicha ley en sus arts. 31 y 32, ya que éste último establece como delitos tipificados y reprimidos con pena de prisión, en los arts. 117 bis y 157 bis del Código Penal la inserción de datos falsos o el proporcionarlos, como el acceder de forma ilegítima o violando los sistemas de confidencialidad y seguridad o revelando a otro la información registrada.

Por ello consideramos indispensable que la ejecución de la historia clínica electrónica se realice bajo los mejores protocolos y mecanismos de seguridad informáticos existentes que son los

criptográficos, que utilizan técnicas como encriptación, firma digital y “time stamping”, que es el sellado digital de fechas, todo lo que garantiza la autoría y brinda fecha cierta de los documentos digitales.

En este punto coincidimos con Vitolo, F. quien ha expresado:

Una de las formas más efectivas para proteger la información consiste en aplicar técnicas de “encriptamiento” a la información contenida en los archivos. Esta técnica, mediante los denominados “algoritmos”, transforma el texto en símbolos ilegibles, impidiendo de esta forma su lectura y su adulteración. Sin embargo, dicho texto “encriptado” se puede recuperar cada vez que sea necesario mediante técnicas de desencriptamiento, que entran en juego cuando ingresa al sistema un usuario autorizado. (Vitolo, 2009).

Finalmente, será imprescindible poner en marcha el organismo de control creado por la legislación especial, a fin de que se encargue de evaluar rigurosamente si las plataformas y demás tecnologías que se van a aplicar para las historias clínicas electrónicas, cumplen con los requisitos de seguridad antes de su uso. Debiendo para ello establecer protocolos exhaustivos de control de riesgos informáticos, como así también una serie de salvaguardas tanto preventivas, como de recuperación de datos y expulsión de los ciber-atacantes de las bases de datos.

Lo anteriormente dicho cobra especial relevancia para el caso de los pacientes amparados por la ley Nacional de respuesta integral al VIH, Hepatitis virales, otras ITS y TBC, dado que su derecho a la confidencialidad se encuentra maximizado, por lo que debe crearse protocolos específicos de disociación de datos, dado que pueden acceder a prestaciones especiales sin necesidad de declarar su diagnóstico, lo que deberá tenerse especialmente en cuenta.

Como corolario podemos decir, que el principio de autonomía del paciente y sus derivados que son el derecho a la confidencialidad de su información sanitaria y al consentimiento informado,

se verán seriamente comprometidos si la historia clínica electrónica no se aplica bajo estrictos protocolos de seguridad y atendiendo a los principios de la ética biomédica que aquí hemos estudiado, puesto que ante la existencia de lagunas legales, debemos recurrir a ellos a modo de brújula normativa.

Bibliografía

Basterra, M. I. (s.f.). La autonomía como derecho fundamental de los pacientes. https://www.salud.gob.ar/dels/entradas/la-autonomia-como-derecho-fundamental-de-los-pacientes

J. Antomás, S. Huarte del Barrio. (s.f.). Confidencialidad e historia clínica. Consideraciones ético-legales. Anales del Sistema Sanitario de Navarra. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1137-66272011000100008

Maliandi, R. (2002). Ética y Biotecnología: cuestión de principios. https://agoraphilosophica.com/Agora5-6/agora5-6-Maliandi.pdf

Reboredo, J. M. (2016). El principio de autonomía y su relación con los principios cardinales de la ética convergente de Ricardo Maliandi. Actas de las XV Jornadas Nacionales sobre Ricardo Maliandi, su vida y sus obras (págs. 156- 166). https://www.aadiebaires.com.ar/pdf/Ricardo%20Maliandi-Actas%20de%20las%20XV%20Jornadas%20Nacionales%20Agora%20Philosophica%202015.pdf

Siurana Aparisi, J. C. (2010). Los principios de la bioética y el surgimiento de una bioética intercultural.

https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-92732010000100006

Vitolo, F. (2009). Aspectos médico-legales de la Historia Clínica Electrónica. https://colpsibhi.org.ar/sites/colpsibhi/files/boletines/aspectos_medico__legales_de_la_historia_clinica_electronica.pdf

Fuentes de información:

Ley 25.326. Protección de datos personales.

Ley 26.994. Código Civil y Comercial de la Nación.

Ley 26.529. Derechos del Paciente.

Ley Nacional 27.675. Respuesta integral al VIH, Hepatitis virales, otras ITS y TBC.

Disposición 2/2021 de la Superintendencia de Servicios de Salud. Protección de los Datos sensibles.

Ley 27553. Recetas electrónicas o digitales.

Decreto reglamentario 98/2023.

Ley 25.506. Firma Digital.

Ley 25.326. Protección de Datos Personales.

Ley 27.706. Programa Federal Único de Informatización y Digitalización de Historias Clínicas de la República Argentina Historia Clínica Electrónica.

Decreto nro. 393/2023. Reglamentario de la ley 27.706.

Asociación Médica Argentina. (2001). Código de Ética para el Equipo de Salud. https://amamed.org.ar/page/ver/Codigo_de_Etica1ra_Edicion#:~:text=Las%20Comisiones%20Directivas%20de%20la%20Asociaci%C3%B3n%20M%C3%A9dica%20Argentina,Organizaciones%20de%20Salud%2C%20que%20deseen%20adherirse%20al%20mismo.

Asociación Médica Mundial (1981). Declaración de Lisboa Sobre los derechos del Paciente.

Organización Mundial de la Salud. (OMS) (2024). Ethics and governance of artificial intelligence for health. (Etica y Gobernanza de la inteligencia artificial para la salud). https://www.who.int/publications/i/item/9789240084759

Organización Panamericana de la salud (OMS). (2021). Historias clínicas electrónicas y la importancia de cómo documentar.

https://iris.paho.org/bitstream/handle/10665.2/54805/OPSEIHIS21022_spa.pdf?sequence=1