Rev Méd Urug 2018; 34(4):228-233
http://www.rmu.org.uy/revista/proximo/rmu34-4_921-gil-historia.pdf
doi: 10.29193/RMU.34.4.6

Historia clínica electrónica: confidencialidad y privacidad de los datos clínicos

Juan Eduardo Gil Yacobazzo*, María José Viega Rodríguez†

Resumen

El país se encuentra implementando la historia clínica electrónica nacional (HCEN) en un escenario donde cada prestador de salud está obligado a contar con una historia clínica electrónica (HCE) y a intercambiar datos clínicos de las personas que son asistidas.

Este trabajo tiene como objetivo revisar y discutir los aspectos vinculados a la confidencialidad y privacidad de los datos de la historia clínica de las personas en este nuevo escenario.

Se comienza por definir un marco conceptual respecto a la HCE y al sistema de HCEN. Se hace una revisión del encuadre jurídico actual respecto a esta temática, haciendo énfasis en conceptos generales de la privacidad y abordando aspectos específicos vinculados al acceso y la custodia de las historias clínicas.

La implementación del sistema HCEN representa a priori varios beneficios, tanto desde el punto de vista asistencial (paciente y médico) como desde el punto de vista del sistema nacional de información en salud. Para llevar adelante la implementación de la HCEN, fue necesario regular algunos aspectos jurídicos, esto es, los derechos y las obligaciones emergentes del nuevo sistema.

Palabras clave: Registros electrónicos de salud
Confidencialidad
Acceso a la información
Uruguay

Key words: Electronic health records
Confidentiality
Access to information
Uruguay

* Profesor Agregado del Dpto. de Métodos Cuantitativos, Facultad de Medicina, Universidad de la República; Ex coordinador médico de Historia clínica electrónica nacional, Programa Salud.uy, AGESIC, Presidencia de la República.
† Dra. en Derecho y Ciencias Sociales. Escribana Pública. Profesora Adscripta de Derecho Informático y Telemático, Universidad de la República. Asesora Jurídica en Derecho Informático de la Dirección Ejecutiva de AGESIC, Presidencia de la República.
Correspondencia: Dr. Juan E. Gil. Departamento de Métodos Cuantitativos, Facultad de Medicina, Av. General Flores 2125 CP 11800, Montevideo, Uruguay. Correo electrónico: jgil@fmed.edu.uy
No existe en este trabajo conflicto de intereses.
Recibido: 18/5/18
Aprobado: 10/9/18

Introducción

En 2005, con motivo de la 58ª Asamblea de la Organización Mundial de la Salud (OMS), se aprobó la resolución sobre Cibersalud[1], donde por primera vez la OMS reconocía la aportación que para la salud y la gestión de los sistemas de salud supone la incorporación de las tecnologías de la información y comunicación (TIC), entendiéndola como una oportunidad única para el desarrollo de la salud pública. El documento define la e-Salud como *"el uso coste-efectivo y seguro de las tecnologías de la información y comunicación en apoyo de la salud y de los ámbitos relacionados con la salud, incluyendo los servicios de atención sanitaria, vigilancia de la salud, literatura y educación, conocimiento e investigación"*, y afirma que el fortalecimiento de los sistemas de salud a través de la e-Salud *"refuerza los derechos humanos fundamentales aumentando y mejorando la equidad, la solidaridad, la calidad de vida y la calidad en la atención"*[2].

A partir de allí varias organizaciones de salud de nuestro medio comenzaron a tener iniciativas o proyectos de implementación de soluciones TIC, siendo los sistemas de historia clínica electrónica (HCE) los mayormente considerados. Además del cambio de paradigma de registro que ello implicó al personal de la salud, estos proyectos comenzaron también a plantear ciertos desafíos ético-jurídicos debido a los cambios que estos sistemas introdujeron respecto al acceso y resguardo de la información.

A su vez, en el año 2012 se firmó un convenio entre el Ministerio de Salud Pública (MSP), el Ministerio de Economía y Finanzas (MEF) y la Agencia de Desarrollo del Gobierno de Gestión Electrónica y Sociedad de la Información y del Conocimiento (AGESIC), creándose el Programa Salud.uy[3], para llevar adelante una estrategia nacional de implementación TIC en el sector salud del país. El Programa Salud.uy ha tenido, dentro de sus principales objetivos, el desarrollo de un sistema de historia clínica electrónica nacional (HCEN), basado en la definición de una plataforma tecnológica que permita interconectar los distintos sistemas informáticos (léase HCE) de los prestadores de servicios de salud y viabilizar de esta forma el intercambio de datos clínicos de los pacientes en el contexto de una asistencia[4].

Este cambio de soporte de la historia clínica (HC), pasando del papel al electrónico, nos enfrenta por lo tanto a un fenómeno de desmaterialización y a aspectos que toman una mayor relevancia y riesgo en la medida que internet potencializa el alcance y manipulación de la información, como es el caso de la confidencialidad y la privacidad.

Este trabajo tiene como objetivo revisar y discutir los aspectos vinculados a la confidencialidad y privacidad de los datos clínicos de las personas, en este nuevo escenario con HCE en los prestadores de servicios de salud y de un sistema de HCEN que viabiliza el intercambio de las historias clínicas entre prestadores. Se comenzará por definir y describir el marco o encuadre jurídico actual respecto a esta temática, la HCE y el sistema HCEN, para luego abordar los aspectos específicos vinculados al acceso y custodia de los datos clínicos de las personas.

Conceptos de intimidad, privacidad y confidencialidad

A los efectos de distinguir los conceptos de intimidad y privacidad resulta muy ilustrativa la conceptualización realizada por la ley española 5/92, que los definía en los siguientes términos: la intimidad protege *"la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona"*, mientras que la privacidad es el *"conjunto más amplio y global de facetas de la personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazados entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado"*[5]. Por otra parte, la confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO), en la norma ISO/IEC 27002, como *"garantizar que la información sea accesible sólo para aquellos autorizados a tener acceso"*, y es una de las piedras angulares de la seguridad de la información. La confidencialidad también se refiere a un principio ético asociado con varias profesiones (por ejemplo, medicina, derecho, religión, psicología profesional y periodismo; en este caso, se habla de secreto profesional).

A su vez, y desde la perspectiva bioética, França define la regla de confidencialidad como *"el derecho de toda persona a proteger los datos que le pertenecen en virtud de que los considera reservados o restringidos (por pertenecer a la intimidad) o su derecho a limitar la difusión de ciertas informaciones u opiniones emitidas"*[6].

Encuadre normativo actual

Datos de la historia clínica

Un punto de partida para el análisis de esta temática está dado por el hecho de que la información registrada en la HC de una persona es propiedad de esta y es categorizada como "dato sensible" por el artículo 4 literal e) de la Ley N° 18.331[7], debiendo gozar de una protección especial tanto ética como legal; en su artículo 18, se regula especialmente los datos sensibles y en el 19 los datos de salud. Por otra parte, el Decreto N° 414/009[8], en su artículo 4° D) define los datos de salud como: *"Las informaciones concernientes a la salud pasada, presente y*

futura, física o mental, de una persona. Entre otros, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad o a su información genética"[9].

A su vez, la confidencialidad de los datos clínicos en la relación médico-paciente se encuentra amparada en el secreto profesional, mientras que la privacidad está protegida por la Ley N° 18.331. Sin embargo, esta norma también refiere a la confidencialidad en el marco de la privacidad. Por su parte, el Código de Ética Médica[10], en su artículo 20, establece la obligación de confidencialidad del médico. En su artículo 22 se establece el deber de confidencialidad como un deber inherente a la profesión médica que solo podrá ser relevado en los casos establecidos por una ley de interés general o cuando exista justa causa de revelación; el artículo 25 establece la prohibición de publicar información del paciente en medios de comunicación sociales.

Respecto a la seguridad de los datos, el artículo 10 de la Ley N° 18.331 establece que: *"El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado"*. En el artículo 11 de la misma ley se consagra el principio de reserva, estableciendo que aquellas personas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de esta a terceros. El inciso 2° refiere a los casos de tercerización de servicios, cuando las instituciones médicas deben brindar información de sus usuarios para que se preste un servicio determinado, debiendo en este caso contar con un contrato que estipule la confidencialidad, así como la remisión expresa a este artículo[11].

Los dos principios pilares para dilucidar las zonas grises en cuanto a la aplicación de la protección de datos personales son el principio de finalidad y el principio del previo consentimiento informado, regulados en los artículos 8 y 9 de la Ley N° 18.331. El principio de finalidad establece que debe informarse la finalidad para la cual se recaban los datos y deben utilizarse de acuerdo a esta, no estando permitido utilizar los datos para una finalidad diferente. El consentimiento, de acuerdo a la ley, debe ser libre, previo, expreso, informado y documentado. Debemos tener en cuenta que es necesario recabar el consentimiento tanto para el tratamiento de la información como para su cesión. Con carácter general, el consentimiento tiene algunas excepciones, establecidas en la ley referida, referente al tratamiento, la cesión y la transferencia internacional de datos.

Historia clínica electrónica

Los conceptos de confidencialidad y privacidad no deberían variar cuando se cambia de escenario de registro y custodia de la HC, es decir, cuando se pasa del formato papel al electrónico. Se entiende por HCE al conjunto integral de datos clínicos, sociales y económicos, referidos a la salud de una persona, desde su nacimiento hasta su muerte, procesados a través de medios electrónicos, siendo el equivalente funcional de la HC papel, de acuerdo a lo establecido en el reciente Decreto Nº 242/017[12]. Pero lo que sí cambia, y debería adecuarse, son los medios de protección y acceso a los datos clínicos electrónicos almacenados (seguridad), de forma de garantizar la privacidad y confidencialidad de estos en este nuevo escenario.

El citado decreto reglamenta lo previsto por la Ley N° 19.355[13], que en su artículo 466 faculta al Poder Ejecutivo para determinar los mecanismos de intercambio de datos clínicos con fines asistenciales a través del sistema de HCEN, a efectos de garantizar el derecho a la protección de la salud de los habitantes y el acceso a las redes integradas de servicios de salud, de conformidad con lo establecido por la Ley N° 18.211[14].

Sistema de historia clínica electrónica nacional

Como ya fue mencionado anteriormente, el sistema HCEN tiene como cometido principal el promover y mejorar la continuidad del proceso asistencial de los usuarios del sistema de salud, brindándole al médico la posibilidad de acceder a la HC del paciente desde cualquier punto asistencial del sistema de salud. Partiendo de la base que cada prestador de servicios de salud mantuvo su propio sistema de HCE, se debió pensar en una estrategia eficiente de acceso a las HC, basado en estándares, para que todos los sistemas de HCE reconocieran los datos generados en cualquiera de estos sistemas. Dicho de otra manera, la "hoja clínica electrónica" generada en el sistema del *prestador 1* debe quedar accesible para ser leída (en caso de necesidad) por otro médico que esté asistiendo al mismo paciente en el *prestador 2*, y así sucesivamente. Para lograr esto fue necesario, por un lado, desarrollar una plataforma tecnológica que permitiese interconectar los distintos sistemas de HCE de los prestadores de servicios de salud del país; y, por otro lado, encaminar un proceso de unificación y normalización de los contenidos de las HC en base a la utilización de estándares de registro clínico electrónico. Por consiguiente, cuando se menciona HCEN no se hace referencia a un software de HCE único y común a todos los

prestadores, sino a un modelo o sistema federado de intercambio de HC.

Para llevar adelante la implementación progresiva del sistema HCEN fue necesario también adaptar el marco normativo. En este sentido, se aprobó el Decreto N° 242/017, al que ya se hizo referencia, el que establece la obligatoriedad para todas las instituciones con competencias legales en materia de salud, sean públicas o privadas, de llevar una HCE y de utilizar la plataforma HCEN.

Custodia de la historia clínica

La Ley Nº 18.335 [15], en el artículo 20, refiere a las medidas de seguridad de la HCE: *"Es de responsabilidad de los servicios de salud dotar de seguridad a las historias clínicas electrónicas y determinar las formas y procedimientos de administración y custodia de las claves de acceso y demás técnicas que se usen. El Poder Ejecutivo deberá determinar criterios uniformes mínimos obligatorios de las historias clínicas para todos los servicios de salud"*.

En el escenario del sistema HCEN, los documentos clínicos electrónicos (DCE) quedarán guardados en la institución donde fueron generados, es decir, donde el paciente fue atendido, y por lo tanto en custodia de esta. Con el fin de identificar dónde se encuentra alojado cada DCE, cada acto o evento asistencial es registrado e indexado en un único índice nacional que se aloja en la plataforma del sistema HCEN. De esta forma, el contenido clínico (lo escrito por el personal de salud) permanecerá siempre en custodia de la institución donde fue generado. Dicho índice nacional de documentos clínicos permite a cada médico actuante, y desde cualquier punto del sistema de salud, consultar alguna atención previa del paciente. Planteado de esta forma, el escenario de la HCEN no sería diferente al actual respecto al concepto de custodia de la HC, donde cada prestador de salud es responsable de la generada en su institución. Esto también implica, y cabe destacarse, que no habrá un repositorio centralizado de documentos clínicos electrónicos.

Acceso a la historia clínica

La Ley N° 18.335, en el artículo 18, establece que todo paciente tiene derecho a conocer lo relativo a su enfermedad. Esto comprende el derecho a que se lleve una HC completa, escrita o electrónica, donde figure la evolución de su estado de salud desde el nacimiento hasta la muerte. Por otra parte, instituye que el paciente tiene derecho a revisar su HC y a obtener una copia de esta a sus expensas, y en caso de indigencia le será proporcionada al paciente en forma gratuita.

En el caso de que una persona cambiase de institución o de sistema de cobertura asistencial, la nueva institución o sistema deberá recabar la HC completa previa del usuario. Este artículo regula en forma expresa que solo podrán acceder a la HC los responsables de la atención médica y el personal administrativo vinculado con estos, el paciente o en su caso la familia y el Ministerio de Salud Pública cuando lo considere pertinente. Finalmente, indica que revelar su contenido, sin que fuere necesario para el tratamiento o mediare orden judicial, o conforme con lo dispuesto por el artículo 19 de la ley, hará pasible del delito previsto en el artículo 302 del Código Penal.

De acuerdo a lo expresado, los datos de salud son considerados "sensibles" y por lo tanto deben quedar "a resguardo" en algún sitio. Hasta el momento, las HC en papel quedan generalmente a resguardo en las Áreas de Registros Médicos (también conocido como Archivo médico) de los distintos prestadores de salud. En ausencia de HCE, la HC papel debe ser extraída de dicha área para permitir al personal asistencial consultarla y registrar en ella. Estos casos responden en su mayoría a la atención en policlínica, la atención durante la internación y eventualmente la atención en los servicios centralizados de emergencia. Otra situación se observa cuando la HC pasa a la dirección técnica de la institución para autorización de algún estudio, entre otros. Pero en todas estas situaciones, quien consulta la HC es el médico que está asistiendo al paciente en ese momento y cuenta con el consentimiento del paciente para hacerlo. Todas estas situaciones refieren a escenarios donde siempre el acceso a la HC se produce en el contexto de una asistencia. Por fuera de estas situaciones, existen otras "no asistenciales", pero donde se requiere una solicitud especial, sea por petición de la Justicia (como documento médico-legal) o de la autoridad sanitaria (Ministerio de Salud), para acceder a la HC. Estas situaciones están claramente definidas respecto a su alcance en la normativa vigente (Ley N° 18.331, Ley N° 18.335 y Decreto N° 242/017).

En el contexto de la HCE estos conceptos que acaban de ser mencionados no deberían diferir, es decir que el personal autorizado del equipo asistencial debería poder acceder a la HC de un paciente en el contexto de su asistencia y durante el período definido por esta. Viéndolo a través de un ejemplo, supongamos que un paciente "pide hora" en su prestador para consultar al *Dr. Fulano* en policlínica. Recién al momento de comenzar con la atención del paciente, el *Dr. Fulano* podría tener acceso a la HC (para consulta de antecedentes, consultas previas, registro del acto, indicaciones y cierre del episodio) y solo durante el lapso de esta. La posibilidad de restringir el acceso, abriendo la posibilidad de solo hacerlo durante la "ventana temporal" de la consulta, es posible ahora en los sistemas de HCE, permitiendo incluso la trazabili-

dad del acceso en caso que fuera necesario. En estos casos, la institución responsable del sistema de HCE será la que tenga la obligación de gestionar adecuadamente los permisos de acceso al sistema para los integrantes del equipo de salud de esta.

Pasando ahora al escenario de la HCEN, supongamos que una persona tiene un accidente en la vía pública y es visto por una emergencia médica móvil. En ese momento, el médico de la móvil actuante, una vez identificado el paciente, podría tener acceso a consultar toda su HC, siempre y cuando medien los permisos y consentimiento correspondientes. De esta forma, a través del índice de documentos electrónicos de la plataforma, cualquier médico en contexto asistencial podría llegar a consultar, desde cualquier punto asistencial del sistema de salud, los distintos documentos clínicos de una persona independientemente de donde hayan sido generados.

En el caso del acceso a la HC con fines de investigación, la institución deberá prever los mecanismos necesarios para impedir el acceso a los datos fuera del contexto asistencial, dado que para ello se requiere del consentimiento de la persona. Cada trabajo de investigación, tanto clínica como epidemiológica, deberá ser presentado ante un comité de ética en investigación en forma previa a su realización y deberá contar con la descripción exhaustiva de la metodología a utilizar para el acceso y recolección de los datos, así como el formulario de consentimiento informado en caso de ser necesario. Será de resorte de cada comité de ética en investigación evaluar la factibilidad de llevar a cabo el trabajo, de acuerdo a si cumple con los requerimientos sobre el manejo y preservación de la confidencialidad de la información recogida. Para estos casos rige lo previsto en el Decreto N° 379/008 de 4 de agosto de 2008[16], que regula el consentimiento libre e informado, enumerándolo como uno de los principios éticos en el capítulo II, punto 4). En el capítulo III establece las formalidades en cuanto a recabar el consentimiento, estableciendo una serie de excepciones, que entendemos están derogadas por la Ley N° 18.331, en virtud al rango legal de la norma y a la fecha de su aprobación. Por lo tanto, las excepciones al principio del consentimiento serán las establecidas en esta ley.

Acceso a la plataforma HCEN

El artículo 18 del Decreto N° 242/017 regula la gestión de acceso a la plataforma de HCEN, estableciendo que las instituciones con competencias legales en materia de salud, públicas y privadas, para acceder a la Red Salud y a la plataforma de HCEN deberán estar debidamente identificadas en forma electrónica. También deberán garantizar a través de mecanismos informáticos seguros la autenticación de las personas cuyo acceso autorizan, así como la privacidad y la integridad de la información clínica intercambiada de forma tal que no sea revelada ni manipulada por terceros. En los artículos 19, 20, 21 y 22 se regula el proceso de intercambio, estableciéndose a texto expreso quiénes podrán acceder a la plataforma.

De todas formas, vale aclarar que a nivel de la plataforma HCEN, no existe ningún dato de tipo "clínico", sino datos de tipo "administrativo" del acto asistencial en sí, incluyendo principalmente el tipo de consulta (por ejemplo, de emergencia, de policlínica y especialidad, si es un resumen de alta de internación, etcétera), del tipo de cobertura, prestador de origen, etcétera. Los datos catalogados como "clínicos", léase datos de la HC de la persona (lo registrado por el médico o cualquier integrante del equipo asistencial), no quedarán disponibles en la plataforma HCEN, sino en los repositorios o bases de datos del sistema de HCE del prestador de salud, manteniéndose de esta manera el principio de "custodia" previsto por la ley.

Consideraciones finales

La obligatoriedad de la HCE y la implementación del sistema HCEN representan a priori varios beneficios de índole asistencial, tanto para los usuarios del sistema de salud (personas) como para los profesionales de la salud actuantes en el acto o evento asistencial. Este punto es de imponderable relevancia para una mejora de la continuidad y calidad del proceso asistencial.

Por otra parte, el paciente, como titular de la HC, continúa resguardado en su esfera íntima y respecto a su privacidad, amparado por la ley de protección de datos, debiendo otorgar su consentimiento para el acceso a su información de salud.

Por su parte, tanto las instituciones de salud, en su calidad de custodios de las HC, como el equipo médico, deberán garantizar la confidencialidad de la información médica, salvo las excepciones legalmente previstas.

Es importante destacar que la incorporación de las tecnologías al proceso asistencial otorga una serie de ventajas pero no alteran los principios de privacidad y confidencialidad. Más aún, el titular de los datos posee mayores posibilidades de control sobre los accesos que puedan producirse a su información clínica que los que poseía en el ámbito tradicional.

Abstract

The national electronic health record (HCEN) is being implemented in our country, within the framework of a scenario whereby each one of the health providers is obliged to have an electronic health record (EHR) and to exchange clinical data of the patients they assist.

The present study aims to review and discuss aspects in connection with the confidentiality and privacy of da-

ta in the health records of individuals in this new scenario.

To start with, a conceptual framework is defined for the EHR and the HCEN. The current legal approach with regard to this topic is reviewed, emphasizing on general concepts of privacy and addressing specific aspects that have to do with the access and custody of health records.

The implementation of the HCEN system initially represents several benefits, both from the healthcare perspective (patient and physician) and from the viewpoint of the national information system for health. In order to implement the HCEN, it was necessary to regulate a few legal aspects, as the rights and obligations arising in the new system.

Resumo

Atualmente se está implementando no Uruguai, o prontuário eletrônico nacional do paciente (HCEN por seu nome em espanhol), no qual cada prestador de serviços de saúde está obrigado a contar com um prontuário eletrônico do paciente (HCE) e ao intercambio dos dados clínicos das pessoas que atendem.

O objetivo deste trabalho é revisar e discutir os aspectos relacionados à confidencialidade e a privacidade dos dados do prontuário eletrônico dos pacientes nestas novas condições.

Define-se um marco conceitual relativo à HCE e ao sistema de HCEN. Faz-se uma revisão dos aspectos jurídicos atuais relacionados ao tema, com ênfase nos conceitos gerais da privacidade incluindo aspectos específicos vinculados ao acesso e custodia dos prontuários eletrônicos.

A priori a implementação do sistema HCEN apresenta vários benefícios, tanto do ponto de vista assistencial (paciente e médico) como do ponto de vista do sistema nacional de informação em saúde. Para a implementação da HCEN, foi necessário regular alguns aspectos jurídicos como os direitos e as obrigações emergentes do novo sistema.

Bibliografía

1. WHA58.28 eHealth. (Ninth plenary meeting, 25 May 2005 –Committee A, seventh report). En: World Health Organization. Fifty-eighth World Health Assembly, Geneva, 16-25 May 2005. WHO: Geneva, 2005: 108-10.
2. **World Health Organization.** eHealth. Report by the Secretariat. EB115/39 (16 December 2004). WHO: Geneva, 2004: 6 p.
3. **Uruguay. Presidencia de la República.** AGESIC. Memoria 2015. Salud.uy. Montevideo: AGESIC, 2015. Disponible en: https://www.agesic.gu:b.uy/innovaportal/file/4636/1/memoria-anual-2015.pdf [Consulta: 3 mayo 2018].
4. **Viega MJ.** El programa Salud.uy. Desarrollo de la Historia Clínica Electrónica Nacional (Libro de Ponencias). En: Congreso de Derecho e Infomática, XX. Salamanca (19-29 octubre). Salamanca: FIADI, 2016.
5. **Viega MJ, Hernández MJ.** Derecho informático e informática jurídica II. Montevideo: FCU, marzo 2018.
6. **França-Tarragó O.** Fundamentos de la bioética: perspectiva personalista. Buenos Aires: Paulinas HSP, 2008.
7. Ley N° 18.331. Ley de protección de datos personales. Montevideo, 11 de agosto de 2008. Disponible en: https://www.impo.com.uy/bases/leyes/18331-2008 [Consulta: 3 mayo 2018].
8. Decreto N° 414/009. Reglamentación de la ley 18.331, relativo a la protección de datos personales. Montevideo, 31 de agosto de 2009. Disponible en: https://www.impo.com.uy/bases/decretos/414-2009/40 [Consulta: 3 mayo 2018].
9. **Viega MJ, Rotondo F, coords.** Privacidad y tecnología en equilibrio. 2013. Disponible en: www.viegasociados.com [Consulta: 3 mayo 2018].
10. Ley N° 19.286. Creación del marco normativo relativo a la expedición de certificados de defunción. Montevideo, 21 de junio de 2018. Disponible en: http://www.asuo.org.uy/doc/C%C3%B3digo_de_%C3%89tica_final.pdf [Consulta: 3 mayo 2018].
11. **Viega MJ, Nahabetian L, coords.** Los derechos ciudadanos en el gobierno electrónico. Montevideo: 2013. Disponible en: http://agesic.gub.uy/innovaportal/file/3551/1/libro_derechos_ciudadanos.pdf [Consulta: 10 enero 2018].
12. Decreto N° 242/017. Reglamentación del art. 466 de la ley 19.355, relativo a los mecanismos de intercambio de información clínica con fines asistenciales a través del sistema de historia clínica electrónica nacional. Revocación del decreto 396/003. Montevideo, 31 de agosto de 2017. Disponible en: https://www.impo.com.uy/bases/decretos/242-2017/4. [Consulta: 3 mayo 2018].
13. Ley N° 19.355. Presupuesto nacional de sueldos gastos e inversiones. Ejercicio 2015-2019. Montevideo, 19 de diciembre de 2015. Disponible en: https://www.impo.com.uy/bases/leyes/19355-2015. [Consulta: 3 mayo 2018].
14. Ley N° 18.211. Creación del sistema nacional integrado de salud. Montevideo, 5 de diciembre de 2017. Disponible en: https://www.impo.com.uy/bases/leyes/18211-2007/61. [Consulta: 3 mayo 2018].
15. Ley Nº 18.335. Derechos y obligaciones de pacientes y usuarios de los servicios de salud. Montevideo, 15 de agosto de 2008. Disponible en: https://www.impo.com.uy/bases/leyes/18355-2008/1 [Consulta: 3 mayo 2018].
16. Decreto N° 379/008. Apruébase el proyecto elaborado por la Comisión de Bioética y Calidad de Atención, dependiente de la Dirección General de la Salud, del Ministerio de Salud Pública, vinculado a la Investigación en Seres Humanos. Montevideo, 14 de agosto de 2008. Disponible en: http://www.impo.com.uy/bases/decretos-originales/379-2008 [Consulta: 3 mayo 2018].