Vol. 7, Nº 27, 2011 ISSN: 1698-7969

Análisis de Aspectos de Interés sobre Privacidad y Seguridad en la Historia Clínica Electrónica

Alberto Saquero Rodríguez[1], Isabel de la Torre[1], Alejandro Durango Pascual[1]

[1]Escuela Técnica Superior de Ingenieros de Telecomucación. Universidad de Valladolid (España).

Resumen / Abstract

Resumen. *Una de las principales ventajas del uso de la Historia Clínica Electrónica (HCE) es la posibilidad de disponer de la información en cualquier momento y lugar. Para ello es imprescindible dotar de seguridad a todo el conjunto. Esta seguridad pasa por distintos aspectos como el control de acceso, la confidencialidad o la auditoría. Aunque existen soluciones ya desarrolladas es fundamental la estandarización para lograr que los requisitos de privacidad sean garantizados en cualquier plataforma. En el presente artículo se exponen en detalle estos aspectos de seguridad, poniéndolos en relación con los mandatos legales tanto de España como de los Estados Unidos.*

Abstract. *One of the main advantages of using Electronic Health Record (EHR) is the information's availability at any time and place. In order to achieve this, the global security is mandatory. That security has got some important issues such as Access Control, confidentiality, and the audit. Although, there are some solutions already developed, the standardization is vital in order to achieve guaranteed privacy requirements over any platform. In this article, these security issues are shown in detail, relating them to the legal Acts of both Spanish and US law.*

1. Introducción

La Historia Clínica (HC) tal y como se define en la Ley 41/2002 [1], es el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial. En dicha ley, también se establecen los usos de la HC obligando a los facultativos con acceso al deber de secreto.

Estos datos son merecedores de una especial protección como se recoge en la Ley 15/1999 de Protección de Datos [2] que los califica como "especialmente protegidos". Además, para su tratamiento se exige el consentimiento inequívoco del paciente salvo casos de urgencia o riesgo vital.

Una de las ventajas que supondría la implantación de la Historia Clínica Electrónica sería la interoperabilidad entre entidades sanitarias, lo que implicaría una mayor disponibildiad de la información

Una de las ventajas que supondría la implantación del HCE sería la interoperabilidad entre entidades sanitarias lo que implicaría una mayor disponibilidad de la información. Sin embargo, esta aparente ventaja choca frontalmente con la privacidad y puede suponer un serio riesgo para la seguridad [3]. Por lo tanto es imprescindible lograr un compromiso entre interoperabilidad y seguridad. Y es que los requisitos de privacidad se vuelven más complejos precisamente por el acceso de distintas organizaciones al HCE.

Por ello, resulta imprescindible alcanzar un consenso sobre qué información dentro del HCE puede resultar más sensible ante posibles brechas en la seguridad del sistema. Así pues, no es igual de crítico el acceso no autorizado a un análisis de bioquímica sanguínea que a los datos genéticos del paciente [4].

Como ya se ha mencionado antes, los facultativos pueden acceder al HC bajo previa autorización del paciente (salvo casos excepcionales) quedando obligados al deber de secreto. Sin embargo, en [5] se afirma que más de la mitad de los profesionales han accedido alguna vez a la HC de un paciente por curiosidad y que incluso han cedido su clave personal a terceros.

Por todo ello, es obvio que la privacidad en el HCE debe partir de unos requerimientos estandarizados y asumibles por las distintas organizaciones sanitarias del mundo. Estos requerimientos se expondrán en la sección 2 que tratará sobre los diferentes servicios de seguridad y los diversos aspectos que influyen en ella.

En la sección 3 se detallará la legislación aplicable a las cuestiones de privacidad y confidencialidad en el HCE tanto en España como en Estados Unidos atendiendo a la HIPAA (Health Insurance Portability and Accountability Act) y más concretamente a la Privacy Rule y la Security Rule.

En la sección 4 se enunciarán algunas soluciones concretas a los problemas de seguridad, que tan críticos pueden resultar para la viabilidad de una solución de HCE y los mecanismos disponibles para garantizar su cumplimiento.

Y por último, tras un análisis en profundidad de los datos presentados en el presente documento, se enunciarán las conclusiones principales y las líneas futuras de trabajo.

2. Requerimientos de Seguridad

La principal característica de un sistema de HCE que puede comprometer la seguridad es la interoperabilidad [3], ya que un tercero solicita acceso a información médica. Suponiendo un esquema completamente in-

teroperable, la cantidad de entidades que podrían acceder a la HCE es enorme, lo que supone un gran desafío.

Los requisitos que debe satisfacer la HCE son autenticación, autorización, integridad, no repudio, confidencialidad y consentimiento.

Pero desde un punto de vista más aplicado, los asuntos más importantes relacionados con la seguridad son:

- Acceso autorizado.

  Para la implantación de un sistema de acceso autorizado es condición indispensable desarrollar un sistema de identificación tanto de los pacientes como de las instituciones sanitarias [6]. Esta identificación debe ser portable de unas organizaciones a otras. Ésta podría lograrse con un identificador nacional (e.g. NSS o DNI). Sin embargo, puede ocurrir que haya pacientes sin este identificador o incluso que sean foráneos lo que complica enormemente el esquema.

  En cuanto a la autenticación, ésta puede resultar sencilla en un sistema centralizado usando infraestructura de clave pública. Sin embargo en un entorno distribuido surge el problema de como autenticar un acceso externo. Podría emplearse un conocimiento previo del usuario (lo que implicaría un proceso de negociación de credenciales independiente) o emplear un registro central de profesionales con acceso a la HCE regulado por un organismo público [7].

  Por último, hay que tener en cuenta el concepto de autorización y decidir qué profesional puede acceder a cierta información y quién no. Para lograr esto puede emplearse un control de acceso basado en roles o RBAC (Role-Based Access Control). Para ello habría que definir los roles existentes y la política de acceso para cada uno [6]. Existen varios problemas asociados al acceso basado en roles y son: la necesidad de una estandarización internacional, gestionar cambios de rol, algunas tareas pueden no tener una asociación directa con algún rol y también posibles variaciones en las políticas de acceso.

- Confidencialidad

  Para garantizar la confidencialidad en una comunicación se emplean algoritmos de cifrado que pueden ser de clave simétrica o asimétrica. Sin embargo, el problema de la confidencialidad en un entorno distribuido surge porque no es posible que el sistema emisor de la información pueda certificar que la confidencialidad no ha sido comprometida en el extremo receptor [7]. Lo cual, puede suponer un problema legal para la entidad emisora.

  Para lograr un sistema confidencial donde las entidades sanitarias tengan garantía jurídica pueden emplearse registros de auditoría (Audit Logs) que se detallarán más adelante.

- Consentimiento del paciente.

  Idealmente, y de acuerdo a la legislación, los pacientes deben poder permitir o denegar el acceso a la totalidad o parte de su HCE excepto en las situaciones de emergencia previstas. Este consentimiento puede ser explícito o

implícito. Si el consentimiento es explícito los costes de gestión pueden ser muy altos, aunque en según la directiva europea 95/46 se prefiere a poner en riesgo la privacidad del paciente.

Otro asunto a tener en cuenta es si es necesario acceder a la HCE almacenada en una organización desde otra externa a ella. En el caso general, regiría el consentimiento del paciente, sin embargo debe proveerse algún mecanismo que permita esquivar esta restricción en casos de emergencia, tal y como se recoge en el estándar EN 13606-4 [9].

- Relevancia

Aquéllos profesionales que intervengan en el proceso de diagnóstico y tratamiento pueden acceder a la HCE [1]. También puede acceder el personal de administración siempre que esté relacionado con sus propias funciones. Es decir, sólo los trabajadores relevantes en el proceso de asistencia pueden acceder a la HCE. Para garantizar este derecho en un sistema automatizado de HCE debe implantarse un registro de acceso o Audit Log. Pero la relevancia de la información es difícil de establecer a priori. Así que se prefiere un acceso más permisivo por defecto y en caso necesario, estudiar posibles abusos a posteriori.

- Propietario de la información.

Ya que el propietario de la información en la HCE está sujeto a distintas obligaciones es necesario establecer quién las asume. La propiedad de la información está ligada al origen de la misma. En la ley 41/2002 se fija como responsables de la información a los facultativos, sin embargo también se refleja el derecho de los pacientes a acceder a su historia clínica [1]. En cuanto a la propiedad de la misma no hay establecido ningún criterio común y es todavía objeto de debate.

- Consistencia de la información.

En un esquema de interoperabilidad debe proveerse de un mecanismo de notificación de correcciones. Estas correcciones deben reflejarse en el Audit Log. Además debe ser capaz no sólo de obtener la versión más reciente de una HCE sino poder volver a versiones anteriores si fuese necesario. Esto implicaría el uso de identificadores unívocos sobre las distintas versiones [7].

En cuanto a las notificaciones de cambio, debe asegurarse no sólo la integridad de los datos sino la advertencia a los médicos implicados de que han podido basar su diagnóstico en una información incorrecta.

- Auditoría.

El registro de auditoría debe incluir todos los accesos, escrituras o modificaciones que tengan lugar sobre la HCE y quién los llevó a cabo. De esta forma cumple con las funciones de monitorización de accesos y permite refinar las políticas de acceso basadas en roles. En definitiva, supone una herramienta muy potente para garantizar un servicio de seguridad de no repudio. Es indispensable para ofrecer este servicio, emplear una referencia temporal común para or-

denar el acceso y poder volver a situaciones pasadas.

Puesto que el registro de auditoría también es distribuido es fundamental cumplir con las exigencias de interoperabilidad. Además, con el fin de no sobrecargar el sistema de HCE, el registro debe estar separado de él.

- Archivado.

Ya que se trata de un sistema distribuido, el proceso de archivado consistiría en almacenar los datos, que por su antigüedad ya no son tan relevantes en el proceso clínico, durante el tiempo estipulado en la legislación (5 años en España).

Para llevar a cabo un archivado satisfactorio puede resultar útil el empleo de niveles de detalle y procesos de resumen automático que están sin definir.

El hecho de que los datos puedan ser borrados tras el período legal choca frontalmente con las líneas futuras de desarrollo de la HCE. Éstas se caracterizan por buscar la consecución de un sistema que recoja los datos clínicos relevantes durante toda la vida del paciente. Y para lograrlo es condición sine qua non disponer de almacenamiento a largo plazo.

3. Legislación Aplicable a la HCE

Como ya se ha mencionado, las principales normas aplicables a la HCE en el ordenamiento jurídico español son la ley 41/2002, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Y también la ley 15/1999 de Protección de Datos de Carácter personal.

En el artículo 9 de la ley 15/1999 se establece textualmente que: "no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad" [2].

Por consiguiente, se deduce que la garantía de seguridad del sistema de HCE no es una cuestión baladí sino que responde a imperativo legal.

De igual modo, en la ley 41/2002 quedan establecidos en el artículo 16 los usos de la historia clínica y la obligatoriedad de separar los datos de identificación personal con los de carácter clínico-asistencial en pos de garantizar el anonimato. Además, en el artículo 18 se establece el derecho del paciente al acceso a su historia clínica siempre que no suponga un perjuicio a terceras personas, como los médicos, a causa de las anotaciones subjetivas que estén reflejadas.

En el artículo 9 de la ley 15/1999 se establece que no se registrarán datos de carácter personal en ficheros que *no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad*

Otro apartado destacable de esta ley es la disposición adicional tercera sobre coordinación de las HC: "El Ministerio y las Comunidades Autónomas promoverán la implantación de un sistema de compatibilidad que posibilite su uso por los centros asistenciales de España".

Algo que no se cumple en el caso de la HCE como se concluye en [3].

En el ámbito internacional de la legislación sobre

privacidad y seguridad es interesante el caso estadounidense. La ley que regula la privacidad y la seguridad de los datos clínicos es la HIPAA (Health Insurance Portability and Accountability Act). Dentro de esta norma existen dos apartados dentro del título II que regula el abuso en los cuidados sanitarios: la regla de privacidad y la regla de seguridad.

La regla de privacidad establece que los datos sanitarios protegidos o PHI (Protected Health Information) sólo pueden ser revelados por orden judicial, para llevar a cabo el tratamiento de la persona o mediante autorización expresa de ésta [10]. Además, esta revelación debe ser la de la menor cantidad de datos necesarios (un principio que también está establecido en la ley 15/1999 de protección de datos).

La regla de seguridad está desarrollada para hacer frente a los retos que supone la digitalización de los datos y el empleo de la Historia Clínica Electrónica

La regla de seguridad fue adoptada en el año 2003 y complementa a la de privacidad. Está especialmente desarrollada para hacer frente a los retos que suponen la digitalización de los datos y el empleo de la HCE. Establece tres tipos de garantes de seguridad: administrativo, físico y técnico [11].

La salvaguarda administrativa son una serie de políticas y procedimientos para ajustarse a los niveles de seguridad requeridos. Especialmente singular es la creación de un agente de privacidad responsable del cumplimiento de las políticas de seguridad y de que los accesos a la HCE los realicen personas autorizadas. También exhorta la creación de un plan de actuación frente a emergencias y la auditoría interna para detectar violaciones de seguridad [11].

La salvaguarda física se centra en el control del acceso físico a los datos protegidos, limitando la manipulación de hardware y software a personal autorizado. Para ello se desplegarán registros de mantenimiento y visitas [11].

La salvaguarda técnica controlará el acceso a los sistemas telemáticos y permitirá a las instituciones sanitarias proteger sus comunicaciones sobre redes públicas [11]. Es más, obliga a la encriptación de datos sobre este tipo de redes. También hace responsables a las instituciones de fallos en la integridad de los datos que puede estar garantizada a través del uso de firma digital entre otros. Además, de cara a la autenticación, las entidades deben poder autenticar a terceras con las que establezcan comunicación mediante contraseña u otros. Por último, les obliga a documentar toda la configuración y a llevar a cabo un programa de análisis y gestión de riesgos.

Más adelante, en el año 2009, estas reglas fueron extendidas en lo que se denomina la HITECH Act [12]. Ya no sólo estaban incluidas en la HIPAA las entidades de provisión de servicios de salud, sino que se extendían las obligaciones a las empresas asociadas a ellas.

Otro aspecto destacable de esta nueva norma es la obligación de notificar al departamento de salud y servicios humanos, potenciales compromisos de la seguridad que hayan tenido lugar.

Por último, reduce el tiempo máximo de retención de datos revelados de la HCE de 6 a 3 años. Esta medida entró en vigor el pasado 1 de enero.

4. Estándares y Soluciones

El estándar europeo 13606 se divide en 5 partes siendo la cuarta dedicada a los aspectos de seguridad. En este estándar se definen las políticas de acceso a los HCE

que podrían considerarse básicas. Están recogidos y regulados aspectos ya expuestos como el consentimiento informado o la seguridad en las comunicaciones.

Por otro lado, es ampliamente utilizado el estándar HL7. En [13] están detallados todos los servicios de seguridad y su consecución mediante protocolos externos a este estándar de nivel de aplicación. Pueden resumirse en la Tabla 1.

Servicios de Seguridad	Mecanismos de Seguridad	
	Técnicas Asimétricas	Técnicas Simétricas
Identificación y Autenticación	Firma Digital	Encriptación, Comprobación de Integridad (MAC)
Autenticación del origen de los datos	Firma Digital, Comprobación de integridad, TVP (Time Variant Parameter), Centro de Confianza.	Encriptación, integridad simétrica (MAC), Centro de Confianza
Integridad	Firma Digital	Encriptación, integridad simétrica (MAC)
Confidencialidad	Auditoría de Seguridad (Identificadores unívocos, informes, etc.)	
Responsabilidad	Auditoría de Seguridad (Identificadores unívocos, informes, etc.)	
No Repudio	Firma Digital, sellos temporales, Centro de Confianza.	Encriptación, integridad simétrica (MAC), sellos temporales, Centro de Confianza.

Tabla 1: Servicios y mecanismos de seguridad (elaboración propia a partir de [13]).

En [8] se realiza una revisión de las soluciones a las que han llegado distintos investigadores destacando tres de ellas por su relevancia con los apartados anteriores: Cassandra (con acceso RBAC), Audit Logic (implementa control de acceso a posteriori y registros de auditoría) o Indivo (que cumple con la normativa HIPAA).

5. Conclusiones y Líneas Futuras

En este artículo se han introducido distintos aspectos relevantes sobre la privacidad y la seguridad en la HCE. Ha quedado patente la necesidad de garantizar los servicios de seguridad expuestos incluso por mandato legal. Igualmente, se ha podido comprobar como este asunto es de actualidad y es una prioridad para todos los países que ven como la generalización de un sistema distribuido de HCE puede suponer una vulneración de la privacidad de los pacientes.

También, se han presentado algunas soluciones concretas que tienen por leitmotiv principal alcanzar los niveles de seguridad requeridos. Sin embargo, el problema principal es la falta de armonización internacional. Ya que la salvaguarda de la privacidad sólo podrá llevarse a cabo en un sistema de HCE real si se alcanza la plena interoperabilidad.

Y por último, plantear como futura línea de actuación el seguimiento y estudio de las nuevas soluciones de HCE para entornos distribuidos que vayan surgiendo. Siempre teniendo presente todos los mandatos legales que aquí se han expuesto y los que en los próximos años se aprobarán.

Referencias

[1] Ley 41/2002 de 14 noviembre, "básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica", BOE 274 Sec. 1, pp. 40126-40132.

[2] Ley 15/1999 de 13 de diciembre "de Protección de Datos de Carácter Personal", BOE 298 Sec. 1, pp. 43088-43099.

[3] B. Sainz de Abajo, I. de la Torre Díez et al., "Evolución, beneficios y obstáculos en la implantación del Historial Clínico Electrónico en el sistema sanitario", RevistaeSalud, Vol.6, Nº22 2010.

[4] A. L. McGuire et al., "Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider", Genetics in Medicine Vol. 10 Nº7, Julio 2008.

[5] M. Iraburu, "Confidencialidad e intimidad", Anuario del Sistema Sanitario de Navarra Vol. 29 Supl. 3, 2006.

[6] David F. Ferraiolo and D. Richard Kuhn, "Role-Based Access Control", 15th National Computer Security Conference (1992) Baltimore, Oct 13-16, 1992. pp. 554 - 563

[7] H. van der Linden et al., "Inter-organizational future proof EHR systems. A review of the security and privacy related issues", International Journal of Medical Informatics 78, pp. 141-160, 2009.

[8] J.L. Fernández Alemán, P.A. Oliver Lozoya, "Seguridad y privacidad en historiales clínicos electrónicos: una revisión de la literatura", RevistaeSalud Vol.6, Nº23, 2010.

[9] Health Informatics - Electronic Health record communication-Part4: Security requirements and distribution rules, CEN/TC 251EN13606-4,2007.

[10] U.S Department of Health & Human Services, "Privacy Rule",http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html, accedido el 28 de mayo de 2011.

[11] U.S Department of Health & Human Services, "Security Rule",http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html, accedido el 28 de mayo de 2011.

[12] U.S. Department of Health & Human Services, "HIPAA Administrative Simplification Statute and Rules", www.hhs.gov, accedido el 6 de marzo de 2011.

[13] B. Blobel, "Standard Guide for EDI (HL7) Communication Security", version 1.1.

FeSalud
Fundación para la eSalud

RevistaeSalud.com es una publicación electrónica que intenta promover el uso de TICs (Tecnologías de la Información y las Comunicaciones) con el propósito de mejorar o mantener la salud de las personas, sin importar quiénes sean o dónde estén.

Edita: FESALUD – Fundación para la eSalud
Correo-e: cperez@fesalud.org
ISSN 1698-7969

SOME RIGHTS RESERVED

Los textos publicados en esta revista, a menos que se indique lo contrario, están sujetos a una licencia de Reconocimiento-NoComercial-SinObraDerivada 2.5 de **Creative Commons**. Pueden copiarse, distribuirse y comunicarse públicamente, siempre que se citen el autor y la revista digital donde se publican, RevistaeSalud.com. No se permite su uso comercial ni la generación de obras derivadas. Puede consultarse la licencia completa en:
http://creativecommons.org/licenses/by-nc-nd/2.5/deed.es