Seguridad y Privacidad en Historiales Clínicos Electrónicos: una Revisión Sistemática de la Literatura

Inmaculada Carrión Señor[1], José Luis Fernandez Aleman[2], Ambrosio Toval Álvarez[3], Pedro Ángel Oliver Lozoya[1]

[1]Grupo de investigación de Ingeniería del Software de la Facultad de Informática de la Universidad de Murcia (España); [2]Doctor en Ingeniería Informática y Profesor Titular en la Universidad de Murcia (España); [3]Catedrático por la Universidad de Murcia y líder del grupo de investigación de Ingeniería del Software de la Universidad de Murcia (España).

Resumen / Abstract

Resumen. *Este trabajo presenta los resultados de una revisión sistemática de la literatura (RSL) relacionada con aspectos de seguridad y privacidad de Historias Clínicas Electrónicas (HCE) e identifica qué enfoques de auditoría de HCEs existen. Se extrajeron 605 artículos usando una cadena de búsqueda predefinida y se revisó el resultado de la misma por parte de tres autores, mientras que otro comprobó dicha revisión. Se seleccionaron 24 artículos, de los cuales, 17 mencionaban estándares, la mayoría relacionados con la privacidad y protección de datos de HCE. Diez de los estudios señalan que se deben encriptar los HCEs. Cuatro trabajos proponen el uso de la técnica del pseudoanonimato para mantener la privacidad del paciente. Tres de los artículos proponen usar un esquema de firma digital para garantizar la autenticidad e integridad de los datos. Finalmente, once de los estudios incluidos consideran necesario realizar una pista de auditoría del sistema. En los últimos años se han diseñado estándares y promulgado directivas que intentan conseguir una mayor homogeneidad de los sistemas de HCEs y lograr de esta forma que los sistemas de HCEs sean interoperables. Sin embargo, los desarrolladores de la mayoría de los sistemas de han definido su arquitectura basándose en los estándares actuales, y esto está suponiendo un agravante a la ya de por sí difícil tarea de conseguir la interoperabilidad de los sistemas de HCEs.*

Abstract. *This study reports the results of a Systematic Literature Review (SLR) related to security and privacy of Electronic Health Records (EHRs) and identifies what EHR audit approaches exist. We extracted 605 articles using a predefined search string and review the outcome of this by three authors, while another checks it. In total, we selected 24 papers, of which 17 mentioned standards, the most of them were related to privacy and security of EHR data. Ten studies mention that EHRs must be encrypted. Four studies propose the use of pseu-*

doanonymity technique to maintain patient's privacy. Three articles propose to use a digital signature scheme to guarantee data authenticity and integrity. Finally, eleven review studies perform a system audit-log. In recent years standards have been designed and directives have been promulgated in order to reach homogeneous EHR systems and, therefore, interoperable EHR systems. However, EHR systems have not been defined using the actual standards and this hinders the interoperability of them.

1. Introducción

Actualmente existe un gran interés en pasar de historiales clínicos escritos en soporte papel a Historiales Clínicos Electrónicos (HCEs). Estos esfuerzos están siendo realizados, principalmente, por las propias organizaciones de forma independiente. Sin embargo, propuestas recientes indican que integrar historiales clínicos proporciona muchos beneficios. Algunos de estos beneficios son: integridad de la información de los HCEs, resistencia a los fallos, alta disponibilidad y consistencia de las políticas de seguridad [1]. Según un estudio realizado en [2] existen cuatro grandes obstáculos que limitan la implantación de los HCEs: financieros, tecnológicos, de actitud ante los HCEs y organizaivos. Muchos gobiernos apoyan esta propuesta debido a los beneficios esperados. El presidente Bush, en 2004, determinó que la mayoría de los americanos estarían conectados a historiales clínicos electrónicos (HCEs) para 2014 [3]. Después, Barack Obama firmó en febrero de 2009 la Ley de Recuperación y Reinversión Americana, en la que incluía la inversión de 19.000 millones de dólares para digitalizar los historiales clínicos de EEUU [4]. También en la Unión Europea (UE) se ha conseguido, tal y como anunció la vicepresidenta de la Comisión Europea y responsable de Agenda Digital, Neelie Kroes, en la Conferencia de Alto Nivel sobre e-Health 2010, que los países integrantes de la UE hagan compatibles sus sistemas de salud antes del 2015, con el fin de compartir los datos y la historia clínica de sus pacientes de forma que se garantice el "libre movimiento" y se pueda realizar una atención sanitaria de calidad y eficiente [5]. Además, comunidades como openEHR [6] y Health Level Seven International (HL7) [7] están intentando desarrollar estándares que unifiquen la atención sanitaria en sistemas de HCEs. Muchas compañías, tales como Google y Microsoft también están intentando proporcionar tales servicios a través de Google Health y Microsoft HealthVault, respectivamente [8].

En 2004, el presidente Bush determinó que la mayoría de los americanos estarían conectados a historiales clínicos electrónicos (HCEs) para 2014

Sin embargo, debido a la mejora en los últimos años de las tecnologías de la información y la comunicación, han surgido nuevas amenazas que planean sobre la seguridad y privacidad de la información de los pacientes [9]. Existe una preocupación real sobre el nivel de accesibilidad de otras personas o entidades a sus HCEs. De echo, los estándares de openEHR [6] y Health Level Seven International (HL7) [7] tratan estos aspectos. El HCE de un paciente puede estar disperso y accesible en varios lugares (por haber acudido a diferentes consultas de especialistas, hospitales, proveedores, etc.), y los defectos de seguridad en alguno de estos sistemas podrían ocasionar que esta información termine siendo revelada a personas o empresas no autorizadas. Por esto, los datos de salud necesitan ser protegidos contra posibles manipulaciones, accesos no autorizados o abusos. Se debe tener un especial cuidado con la

protección de datos, incluyendo confidencialidad, integridad, autenticación, responsabilidad y disponibilidad, por lo que se debe ser muy riguroso en las actividades de almacenamiento e intercambio de información, especialmente en el desarrollo e implementación de los HCEs. Además, los sistemas de EHR deben tener un método para comprobar la calidad de los mismos. Por ejemplo, una lista de requisitos.

El objetivo de este trabajo es realizar una Revisión Sistemática de la Literatura (RSL) existente en relación con los aspectos de seguridad y privacidad de los HCEs. Se trata de una revisión nueva y su objetivo es responder a las siguientes preguntas:

Q1 *¿Que características de seguridad y privacidad presentan los actuales sistemas de HCEs?* Se intentará analizar en profundidad todos los aspectos más relevantes relacionados con la privacidad y seguridad que presentan los actuales sistemas de HCEs.

Q2 *¿Qué enfoques de auditoría en HCEs existen?* Se identificarán y estudiarán los trabajos que abordan la auditoría de los sistemas de HCEs. Nosotros analizamos dos aproximaciones: la realización de un registro de auditoría del sistema y el diseño de una checklist basada en Ingeniería de Requisitos (IR) que mide la calidad del sistema EHR.

2. Métodos

2.1. Revisión sistemática, protocolo y registro

Los autores usaron métodos formales para la realización de la RSL para asegurar una búsqueda y proceso de recuperación precisos e imparcial. Una revisión sistemática es un método de estudio científico que pretende recopilar toda la investigación sobre un tema determinado, evaluarla críticamente y obtener unas conclusiones que resuman la investigación. El objetivo de una revisión sistemática no es solo agrupar todas las pruebas existentes de una pregunta de investigación, sino apoyar el desarrollo de directrices basadas en pruebas para los profesionales.

2.2. Criterios de inclusión

Se utilizaron los siguientes criterios de inclusión:

- CI1. Artículos publicados en inglés;
- CI2. Fecha de publicación entre enero de 2006 y enero de 2011;
- CI3. Artículos que versen sobre privacidad y seguridad de los HCEs;

Se incluyeron sólo artículos escritos en inglés (CI1) por ser el idioma preferido por la comunidad científica para la publicación de artículos de investigación. Además, se buscan trabajos desde enero de 2006 (CI2) pensando que serán de mayor interés, al ser más actuales y usar las últimas tecnologías, y seguir los estándares publicados en los últimos años, como la Norma CEN/ISO 13606 [10] publicada en 2008 y actualizada en 2010. Por último, los criterios de elegibilidad CI3 y CE1 se incluyen para poder responder las preguntas de investigación planteadas. Por tanto, se descartaron aquellos que trataban únicamente sobre criptografía.

2.3. Fuentes de información

La búsqueda se realizó a través de las bases de datos bibliográficas Medline, ACM Digital Library, Wiley InterScience, IEEE Digital Library, Science@Direct, MetaPress, ERIC, CINAHL y Trip database. La consulta de estas bases de datos se inició en abril de 2009 y terminó 2 en enero de 2011. Además de los artículos encontrados a través de la consulta a estas bases de datos, se revisaron las referencias de los artículos in-

cluidos para que la revisión fuese más exhaustiva.

2.4. Selección de Estudios

La selección de los estudios fue organizada en las siguientes cuatro etapas:

1. Búsqueda de publicaciones en las bases de datos electrónicas relacionadas con la salud y la informática. Para efectuar esta etapa se usó la siguiente cadena de búsqueda: ("electronic Elath record" AND "audit" AND ("privacy" or "security"), adaptándola a las características de los motores de búsqueda de las bases de datos.
2. Exploración de título, resumen y palabras clave de los artículos y adoptación de los criterios de elegibilidad.
3. Lectura completa o parcial de los artículos que no pudieron ser discriminados en el paso anterior, para descubrir si estos encajaban o no en el estudio de acuerdo con los criterios de elegibilidad.
4. Se llevó a cabo un seguimiento de citas y examen detallado de las referencias para encontrar documentos adicionales, que fueron revisados tal y como se indica en los pasos 2 y 3.

Las actividades definidas en las etapas descritas fueron realizadas por los investigadores Pedro Ángel. Oliver, Inmaculada Carrión y José Luis Fernández de manera independiente.

Cualquier discrepancia o duda se resolvió con la consulta a un cuarto miembro del equipo de investigación, Ambrosio Toval.

La selección se desarrolló en un proceso iterativo a través de evaluaciones individuales hasta que se alcanzó una fiabilidad interevaluador aceptable (0.83).

2.5. Proceso de Recopilación de Datos

La recopilación de los datos se llevó a cabo utilizando un formulario de extracción de datos. De cada artículo potencialmente relevante, se evaluó su texto completo por uno de los autores. Por tanto, un único revisor extrajo la información, mientras que otro la comprobó. Los desacuerdos se resolvieron mediante la discusión de los dos autores que revisaron el informe.

2.6. Análisis de Datos

Se diseñó una plantilla con los datos que se debían extraer de cada artículo. Esas características se agruparon en tres categorías:

Generales. Autores, año de publicación, origen editorial, país de procedencia, resumen, aportaciones originales, principales hallazgos, conclusiones y otras aclaraciones.

Respuesta a la pregunta Q1. Estándares aplicados, implantación institucional, mecanismos de privacidad y seguridad en la información.

Respuesta a la pregunta Q2. Existencia de un sistema de auditoría, adopción de un enfoque basado en IR para auditar un sistema de HCEs.

3. Resultados

3.1. Selección de Estudios

Un total de 24 artículos se incluyeron en la revisión. La búsqueda en las bases de datos proporcionó un total de 605 artículos. De ellos, se descartó uno por no estar escrito en inglés (CI1). A continuación, se descartaron 134 por no cumplir el CI2. De los 470 artículos que quedaban, 396 se descartaron tras revisar los títulos, resúmenes y palabras clave que aparecían en dichos artículos al no cumplir con el criterio de inclusión 3

(CI3).

El texto completo de los 74 artículos restantes se examinó completamente. Se descartaron 53 por no cumplir con el CI3, lo que nos deja un total de 21 artículos incluidos en la revisión. Adicionalmente, 3 estudios más se incluyeron tras la revisión de las referencias de estos artículos.

3.2. Características de los Estudios

En este apartado se describirán las características principales de los estudios incluidos en la revisión. Se presentan de manera resumida las características relacionadas con la privacidad y seguridad en los sistemas de Historias Clínicas Electrónicas, los estándares en los que se basan y si realizan un registro de auditoría.

3.2.1. Estándares

En cuanto a los estándares utilizados en los artículos revisados, 17 trabajos (71 %) hablan o se basan en estándares a la hora de mostrar sus estudios. De estos, 13 trabajos (76,47 %) mencionan el Health Insurance Portability and Accountability Act (HIPAA) de 1996 [11, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22], por lo que se convierte en el estándar más utilizado, en el cual se fijan reglamentos relativos a la privacidad en la informática médica en EE.UU. También aparece con relativa frecuencia la Directiva Europea de Protección de Datos 95/46/EC, que se menciona en 4 trabajos (25,53 %) [23, 14, 15, 21]. Esta directiva es relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta directiva es aplicable a la privacidad de los datos personales en general, por lo que también se aplica a los datos incluidos en los HCEs. Otros estándares que aparecen con mucha menos asiduidad son: EuroSOCAP [23], la guía de la Organisation for Economic Cooperation and Development (OECD) sobre protección de datos [23], el Estándar de Control de Acceso Basado en Roles "American National Standard for Information Technology" [24], el "Standard Specification for Continuity of Care Record (CCR) de American Society for Testing and Materials (ASTM) [11], el "Clinical Document Architecture" (CDA) [11, 12] de HL7, el "Continuity of Care Document" (CCD) [11] de HL7 y ASTM, el HL7 Version 3 [25], el CEN/TC215 13606 [25], el ISO TS 22600 [25], el ASTM E1986-98 [25], el ISO DTS 21298 [25], el Recommendations for the Interpretation and Application of the Personal Information Protection and Electronic Documents Act"[16], el Recommendation R (75) de Europa [17], el Privacy Code de Nueva Zelanda [17], el IMIA Code of Ethics for Health Information Professionals [17] y el ISO/IEC 21000-4 [22].

3.2.2. Privacidad y seguridad

Todos los artículos incluidos en este estudio mencionan la privacidad y seguridad en los sistemas de HCEs. Los aspectos más importantes se agrupan a continuación. Un total de 10 trabajos (41,67 %) [26, 4, 12, 15, 27, 16, 17, 18, 19, 28] señalan que los sistemas deben encriptar los HCEs para aumentar su seguridad, aunque J. Choe y S. K. Yoo [27] proponen encriptación selectiva de la información del paciente, de manera que parte de los datos del paciente estarán cifrados y parte no lo estarán, para reducir la carga computacional. Además S. Narayan et al. [16] proponen encriptar tanto el HCE como sus metadatos.

Sólo 4 trabajos [29, 15, 18, 28] proponen la técnica del pseudoanonimato, la cual consiste en mostrar la información sanitaria de un paciente sin revelar la información personal del mismo, por ejemplo, mostrando un identificador en lugar de los datos personales del paciente. De estos últimos, [18, 28] proponen asociar los HCEs a un hash del identificador del

paciente como medida extra de seguridad. El hash del identificador es un token derivado de aplicar una función hash al identificador del paciente. Una función hash asegura that sea muy difícil obtener el identificador del paciente a partir del token. R. Zhang y L. Liu [18] proponen mantener también el anonimato del personal sanitario que accede al HCE, si accede sin permiso explícito del paciente, sino porque otro profesional sanitario que tuviese el permiso de acceso se lo delegue.

Para garantizar la autenticidad e integridad de los datos de los HCEs, [18, 19, 28] proponen utilizar un esquema de firma digital en el que el personal o las instituciones sanitarias firman los datos. Zhang y Liu [18] usan un esquema de firma anónima, llamado grupo de firma, para mantener el anonimato del profesional sanitario concreto que firmó el HCE.

Quantin et al. diseñan un motor de búsqueda en una base de datos distribuida en diferentes instituciones sanitarias, que permite mantener el anonimato del paciente

Es necesario hacer notar que, al permitir al usuario consultar o realizar cambios en los HCEs, se podría detectar un problema de violación de privacidad y seguridad si los datos de acceso del paciente (contraseña o otro mecanismo de acceso) fuesen robados por personas no autorizadas [4, 26]. J. Benaloh et al. [4] proponen un diseño como solución para el almacenamiento seguro y privado de los HCEs de los pacientes, así como un sistema en el que cada paciente conceda acceso a porciones específicas de los datos de su HCE. S. Narayan et al. [16] proponen mejorar la gestión de claves de J. Benaloh et al. usando un esquema de cifrado basado en atributos en un escenario en el que los HCEs estarán almacenados en la nube. Su principal objetivo es asegurar que el proveedor del almacenamiento no pueda acceder a los HCEs. R. Zhang y L. Liu [18] y S. Haas et al. [21] también se plantean que el almacenamiento lo proporcione un proveedor (nube) ajeno al paciente y a las instituciones sanitarias, y consideran importante que el usuario no tenga que confiar en que este proveedor no acceda a sus datos, sino que esté garantizado.

Por otro lado, G. C. Hembro_ y S. Muftic [17] diseñan un sistema en el que los HCEs del paciente se almacenan en las tarjetas inteligentes sanitarias de los mismos. K. Win et al. [13] investigan diferentes sistemas de HCEs y las funciones y problemas de seguridad, como son el acceso y la protección de la información.

En el trabajo de H. van der Linden et al. [25] identifican y analizan la privacidad y la seguridad relacionadas con problemas que se producen cuando la información de salud se intercambia entre las organizaciones sanitarias. J. Sun y Y. Fhan [19] diseñan un sistema de HCEs que permite la compartición de datos entre distintas instituciones del cuidado de la salud protegiendo la privacidad del paciente, mientras que C. Quantin et al. [28] diseñan un motor de búsqueda en una base de datos distribuída entre diferentes instituciones sanitarias, que permite mantener el anonimato del paciente a través de todas las comunicaciones.

M. Jafari et al. [30] proponen usar la gestión de derechos digitales (DRM) para compartir los HCEs entre investigadores. J. Choe y S. K. Yoo [27] proponen una arquitectura multi-agente para el acceso a la información autorizada y el intercambio seguro de la información del paciente basada en servicios Web. Finalmente, en el trabajo de R. Agrawal y C. Johnson [14] se presenta la Hippocratic Database, que es un conjunto integrado de tecnologías que gestiona la revelación de HCEs en conformidad con las leyes de pro-

tección de datos sin impedir el flujo de información de manera legítima. Sin embargo, A. Al Faresi et al. [20] detectan una desventaja en esta base de datos porque trata las políticas de privacidad y las políticas de control de acceso de forma conjunta. Por ello las separan diseñando un controlador de la privacidad.

3.3. Auditoría del Sistema

Once de los trabajos de la revisión (45,83 %) [23, 24, 13, 31, 12, 17, 18, 19, 20, 21, 22] creen necesario conocer quién está accediendo a nuestro historial médico y con qué propósito, por eso creen necesaria realizar una pista de auditoría para obtener esta información. Haas et al. [21] proponen realizar auditorías de los accesos y de todos los flujos de datos, a fin de que el paciente pueda comprobar que las políticas de acceso se están cumpliendo. Tres de los trabajos, [31, 17, 22] indica que auditar los accesos es necesario al soportar la anulación de las políticas de acceso en situaciones de emergencia, para comprobar a posteriori que no se ha hecho un uso malintencionado de los datos accedidos. Además, dos de los artículos [31, 22] proponen utilizar la auditoría para mejorar las políticas de acceso.

4. Discusión

4.1. Resumen de evidencia

En esta sección, se resumirán las principales tendencias extraídas de los estudios incluidos en la revisión que contesten a las preguntas de investigación planteadas:

4.1.1. Q1. *¿Qué características de seguridad y privacidad presentan los actuales sistemas de HCEs?*

En general, la mayoría de los trabajos incluidos en la revisión hablan o se basan en estándares, lo que muestra la necesidad de la utilización de los mismos en sistemas de HCEs que pretendan garantizar la privacidad y seguridad de los datos del paciente. El estándar más referenciado es el HIPAA, utilizado en USA. El HIPAA es una ley federal que protege la información sanitaria del paciente. Otro estándar de gran importancia en Europa, es la Norma CEN/ISO 13606, que incluye en su capítulo cuarto directivas de privacidad y seguridad. Es un estándar incipiente desarrollado por CEN en 2008, aprobado por ISO y actualizado en 2010 y cuyo fin no es imponer cómo se deben realizar los sistemas de HCEs sino proponer unas normas comunes en todos ellos para que de esta manera la interoperabilidad sea posible. A partir de la revisión, se puede observar que aún es escasa la presencia de trabajos de investigación relacionados con la seguridad y privacidad enmarcados bajo la Norma CEN/ISO 13606, pero el uso de estándares que definen reglas de privacidad y seguridad es frecuente.

Para mantener la privacidad del paciente se utiliza la técnica del pseudoanonimato

Para mantener la privacidad y seguridad de los HCEs de los pacientes, una de las medidas preferidas por los autores es la encriptación de los mismos. En la mayoría de los casos, se proponen esquemas de cifrado de clave asimétrica. Para garantizar la integridad y autenticación de los datos, los estudios consultados prefieren que el personal sanitario que crea o modifica el HCE lo firme digitalmente.

Por último, para mantener la privacidad del paciente se utiliza la técnica del pseudoanonimato, sobre todo, en aquellos escenarios en los que el almacenamiento de los HCEs se realiza en la nube, para impedir que el proveedor de dicho almacenamiento pueda tener ningún tipo de información sobre el paciente.

4.1.2. Q2. *¿Qué enfoques de auditoría en HCEs existen?*

Once de los trabajos incluidos en el estudio consideran necesario auditar quién está accediendo a los datos y con qué propósito. La realización de una pista de auditoría es muy importante en los sistemas de HCEs que permiten saltarse las políticas de acceso en situaciones de emergencia y se considera fundamental para que el usuario pueda comprobar que el sistema está ejecutando correctamente todas las políticas de privacidad y acceso definidas. Además, L. Rostad y O. Edsberg [31] y C. A. Ardagna et al. [22] proponen utilizar la auditoría no sólo para detectar un mal uso del sistema, sino para mejorar las políticas de acceso. En la actualidad, realizar una pista de auditoría es uno de los grandes retos, pues existen escasas propuestas que aborden esta problemática.

4.2. Limitaciones de la revisión

Los procedimientos usados en este estudio pueden presentar algunas limitaciones inherentes a una revisión sistemática:

- La búsqueda se organizó como un proceso de búsqueda manual en varias bases de datos científicas específicas. Es posible que durante la revisión realizada, existan palabras que no se hayan encontrado o no se hayan tenido en cuenta (por ejemplo sinónimos de HCEs), por lo que es posible que puedan faltar estudios relevantes.
- Sólo se han incluido artículos en inglés, por tanto, los resultados deben considerarse dentro del ámbito de artículos de este tipo.
- No se han incluido artículos publicados después de la fecha de búsqueda.
- Un investigador extrajo los datos de cada trabajo y otro los comprobó. Los revisores podrían haber pasado por alto información relevante sobre seguridad y privacidad en los HCEs.

4.3. Conclusión

Aunque existen muchas propuestas de sistemas de HCEs, parece que los desarrolladores de los mismos no han definido su arquitectura basándose en los estándares actuales, y esto está suponiendo un agravante a la ya de por si difícil tarea de conseguir la interoperabilidad de los sistemas de HCEs. Afortunadamente, en los últimos años se han diseñado estándares y promulgado directivas que intentan conseguir una mayor homogeneidad de los sistemas de HCEs y lograr así de esta forma que los sistemas de HCEs serán interoperables, lo que favorecería al personal médico, pacientes, administración e investigadores al ahorrar costes, tiempo y esfuerzo.

Es muy importante y necesario realizar un completo análisis de requisitos de seguridad en las herramientas de los sistemas de HCEs. Muy pocos trabajos mencionan este aspecto, tan sólo M. Farzandipour et al. [9] realizan un análisis de requisitos de seguridad pero no es completo ni se basa en ningún estándar. Por ello, se espera realizar un catálogo de requisitos de privacidad y seguridad que deben cumplir las aplicaciones de HCEs. Este se basaría en algún estándar internacional reconocido, como el CEN/ISO 13606. Este catálogo está previsto utilizarlo para auditar aplicaciones de HCEs reales siguiendo métodos similares a los propuestos en [32, 33].

5. Agradecimientos

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia y Tecnología, proyecto PEGASO,

TIN2009-13718-C02-01, PANGEA, TIN2009-13718-C02-02.

Bibliografía

[1] Allard T, Anciaux N, Bouganim L, Guo Y, Le Folgoc L, Nguyen B, et al. Secure personal data servers: a vision paper. Proceedings of the VLDB Endowment. 2010 September;3:25–35.

[2] de Abajo BS, de la Torre Díez I, González PB, Salcines EG, Pernas FJD, Higuera JFD, et al. Evolución, beneficios y obstáculos en la implantación del Historial Clínico Electrónico en el sistema sanitario. Revistae-Saludcom. 2010;6(22).

[3] Hesse BW, Hansen D, Finholt T, Munson S, Kellogg W, Thomas JC. Social Participation in Health 2.0. Computer. 2010 November;43:45–52.

[4] Benaloh J, Chase M, Horvitz E, Lauter K. Patient controlled encryption: ensuring privacy of electronic medical records. In: Proceedings of the 2009 ACM workshop on Cloud computing security. CCSW '09. New York, NY, USA: ACM; 2009. p. 103– 114.

[5] Los países de la UE compartirán historias clínicas antes de 2015 [Internet]. Available from: http://www.europapress.es; 2010. Available from: www.europapress.es.

[6] Beale T, Heard S. OpenEHR Architecture Overview; 2007. Available from: http://www.openehr.org/svn/specification/TRUNK/publishing/architecture/overview.pdf.

[7] HL7; 2009. Available from: http://www.hl7.org.

[8] Sachdeva S, Saphina M, Bhalla S. Web Services Security Issues in Healthcare Applications. In: Proceedings of the 2010 IEEE/ACIS 9th International Conference on Computer and Information Science. Washington, DC, USA: IEEE Computer Society; 2010. p. 91–96.

[9] Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study. Journal of Medical Systems. 2009;.

[10] Norma ISO/CEN 13606; 2010. Available from: www.aenor.es.

[11] Kahn S, Sheshadri V. Medical Record Privacy and Security in a Digital Environment. IT Professional. 2008 March;10:46–52.

[12] Hu J, Chen HH, Hou TW. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards & Interfaces. 2010 October;32:274–280.

[13] Win KT, Susilo W, Mu Y. Personal Health Record Systems and Their Security Protection. Journal of Medical Systems. 2006 August;30:309–315.

[14] Agrawal R, Johnson C. Securing electronic health records without impeding the flow of information. International Journal of Medical Informatics. 2007;76(5-6):471 – 479.

[15] Elger BS, Iavindrasana J, Lo Iacono L, Müller H, Roduit N, Summers P, et al. Strategies for health data exchange for secondary, cross-institutional clinical research. Computer Methods and Programs in Biomedicine. 2010 September;99:230–251.

[16] Narayan S, Gagné M, Safavi-Naini R. Privacy preserving HER system using attribute-based infrastructure. In: Proceedings of the 2010 ACM workshop on Cloud computing security workshop. New York, NY, USA: ACM; 2010. p. 47–52.

[17] Hembro_ GC, Muftic S. SAMSON: Secure access for medical smart cards over networks. In: Proceedings of the 2010 IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). Washington, DC, USA: IEEE Computer Society; 2010. p. 1–6.

[18] Zhang R, Liu L. Security Models and Requirements for Healthcare Application Clouds. In: Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing.Washington, DC, USA: IEEE Computer Society; 2010. p. 268–275.

[19] Sun J, Fang Y. Cross-Domain Data Sharing in Distributed Electronic Health Record Systems. IEEE Transactions on Parallel and Distributed Systems. 2010;21:754–764.

[20] AL Faresi A, Wijesekera D, Moidu K. A comprehensive privacy-aware authorization framework founded on HIPAA privacy rules. In: Proceedings of the 1st ACM International Health Informatics Symposium. New York, NY, USA: ACM; 2010. p. 637–646.

[21] Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller G. Aspects of privacy for electronic health records. International Journal of Medical Informatics. 2011;80(2):e26 – e31.

[22] Ardagna CA, di Vimercati SDC, Foresti S, Grandison TW, Jajodia S, Samarati P. Access control for smarter healthcare using policy spaces. Computers & Security. 2010;29(8):848 – 858.

[23] Falcão-Reis F, Costa-Pereira A, Correia ME. Access and privacy rights using web security standards to increase patient empowerment. Studies in Health Technology and Informatics. 2008;137:275–285.

[24] Röstad L. An Initial Model and a Discussion of Access Control in Patient Controlled Health Records. In: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. Washington, DC, USA: IEEE Computer Society; 2008. p. 935–942.

[25] van der Linden H, Kalra D, Hasman A, Talmon J. Interorganizational future proof EHR systems: A review of the security and privacy related issues. International Journal of Medical Informatics. 2009;78(3):141–160.

[26] Daglish D, Archer N. Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues. In: Proceedings of the 2009 World Congress on Privacy, Security, Trust and the Management of e-Business.Washington, DC, USA: IEEE

Computer Society; 2009. p. 110–120.

[27] Choe J, Yoo SK. Web-based secure access from multiple patient repositories. International Journal of Medical Informatics. 2008;77(4):242–248.

[28] Quantin C, Jaquet-Chi_elle DO, Coatrieux G, Benzenine E, Allaert FA. Medical record search engines, using pseudonymised patient identity: An alternative to centralised medical records. International Journal of Medical Informatics. 2011;80(2):e6 – e11.

[29] Riedl B, Neubauer T, Goluch G, Boehm O, Reinauer G, Krumboeck A. A secure architecture for the pseudonymization of medical data. In: Proceedings of the The Second International Conference on Availability, Reliability and Security. Washington, DC, USA: IEEE Computer Society; 2007. p. 318–324.

[30] Jafari M, Safavi-Naini R, Saunders C, Sheppard NP. Using digital rights management for securing data in a medical research environment. In: Proceedings of the tenth annual ACM workshop on Digital rights management. New York, NY, USA: ACM; 2010. p. 55–60.

[31] Rostad L, Edsberg O. A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs. In: Proceedings of the 22nd Annual Computer Security Applications Conference. Washington, DC, USA: IEEE Computer Society; 2006. p. 175–186.

[32] Martínez MA, Lasheras J, Fernández Medina E, Toval A, Piattini M. A Personal Data Audit Method through Requirements Engineering. Computer Standards & Interfaces. 2010;32(4):166–178.

[33] Martínez MA, Toval Álvarez JA, Campos M. Requirements Engineering to Audit Privacy Issues in Medical and Health Software. In: HEALTHINF (2); 2008. p. 74–81.

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