Gac Sanit. 2012;**26(5)**:463–468

Revisión

Gestión del control de acceso en historiales clínicos electrónicos: revisión sistemática de la literatura

Inmaculada Carrión Señor*, José Luis Fernández Alemán y Ambrosio Toval

Grupo de Investigación de Ingeniería del Software, Departamento de Informática y Sistemas, Facultad de Informática, Universidad de Murcia, Murcia, España

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Recibido el 2 de agosto de 2011
Aceptado el 15 de noviembre de 2011
On-line el 15 de marzo de 2012

Palabras clave:
Registros electrónicos de salud
Historia clínica electrónica
Seguridad
Privacidad
Control de acceso
Tecnología inalámbrica
Revisión sistemática

R E S U M E N

Objetivo: Este trabajo presenta los resultados de una revisión sistemática de la literatura relacionada con aspectos del control de acceso en sistemas de historias clínicas electrónicas, la seguridad en entornos inalámbricos y la formación de los usuarios de dichos sistemas en temas de privacidad y seguridad.
Métodos: Como fuente de información se utilizaron artículos originales encontrados en las bases de datos Medline, ACM Digital Library, Wiley InterScience, IEEE Digital Library, Science@Direct, MetaPress, ERIC, CINAHL y Trip Database, publicados entre enero de 2006 y enero de 2011. Se extrajeron 1208 artículos usando una cadena de búsqueda predefinida, y el resultado fue revisado por los autores. El resultado final de la selección fue de 24 artículos.
Resultados: 21 de los artículos encontrados mencionaban las políticas de acceso a los sistemas de historias clínicas electrónicas . Once artículos discuten si deben ser las personas o las entidades quienes concedan los permisos en las historias clínicas electrónicas. Los entornos inalámbricos sólo se consideran en tres artículos. Finalmente, sólo cuatro citan expresamente que es necesaria la formación técnica de los usuarios.
Conclusiones: El control de acceso basado en roles es el mecanismo preferido para implementar la política de acceso por los diseñadores de historias clínicas electrónicas. El control de acceso es gestionado por usuarios y profesionales médicos en la mayoría de los sistemas, lo que promulga el derecho del paciente a controlar su información. Por último, la seguridad en entornos inalámbricos no es considerada en muchos casos, y sin embargo, una línea de investigación es la eSalud en entornos móviles, conocida como mHealth.

Access control management in electronic health records: a systematic literature review

Keywords:
Electronic health records
Safety
Privacy
Gatekeeping
Wireless technology
Systematic review

A B S T R A C T

Objective: This study presents the results of a systematic literature review of aspects related to access control in electronic health records systems, wireless security and privacy and security training for users.
Methods: Information sources consisted of original articles found in Medline, ACM Digital Library, Wiley InterScience, IEEE Digital Library, Science@Direct, MetaPress, ERIC, CINAHL and Trip Database, published between January 2006 and January 2011. A total of 1,208 articles were extracted using a predefined search string and were reviewed by the authors. The final selection consisted of 24 articles.
Results: Of the selected articles, 21 dealt with access policies in electronic health records systems. Eleven articles discussed whether access to electronic health records should be granted by patients or by health organizations. Wireless environments were only considered in three articles. Finally, only four articles explicitly mentioned that technical training of staff and/or patients is required.
Conclusion: Role-based access control is the preferred mechanism to deploy access policy by the designers of electronic health records. In most systems, access control is managed by users and health professionals, which promotes patients' right to control personal information. Finally, the security of wireless environments is not usually considered. However, one line of research is eHealth in mobile environments, called mHealth.

Introducción

En un esfuerzo por modernizar el sistema sanitario de Estados Unidos, el presidente Bush, en 2004, concluyó que la mayoría de los historiales clínicos electrónicos americanos deberían estar conectados antes de 2015[1]. En esta misma línea, la iniciativa Health Information Technology for Economic and Clinical Health (HITECH) del presidente Obama ha hecho que se despierte un gran interés por las historias clínicas electrónicas. Sin embargo, Estados Unidos muestra un retraso con respecto a la mayoría de los países de la Unión Europea en cuanto a la implementación de este tipo de sistemas. Concretamente en España, cada comunidad autónoma ha desarrollado su propio sistema de historia clínica electrónica, pero con grandes similitudes, y es habitual que las comunidades

* Autora para correspondencia.
Correo electrónico: mariainmaculada.carrion@um.es (I. Carrión Señor).

0213-9111/$ – see front matter
doi:10.1016/j.gaceta.2011.11.019

compartan experiencias y buenas prácticas[2]. Los sistemas de historias clínicas electrónicas pueden proporcionar grandes beneficios, ya que la información de un paciente procede de múltiples organizaciones sanitarias: *1)* se obtiene información completa integrada, *2)* evita duplicidades e inconsistencias; y *3)* hay una alta disponibilidad de los datos[3]. Los aspectos de privacidad y seguridad en los sistemas de historias clínicas electrónicas son de vital importancia. En un trabajo relacionado[3] ya se realizó una revisión sistemática de la literatura en la cual se trataba de extraer las características generales de privacidad y seguridad que siguen los actuales sistemas de historias clínicas electrónicas. En ese trabajo se recogió toda la información pertinente para conocer el estado actual de este campo. Como continuación del estudio anterior, el objetivo de nuestro trabajo es describir en profundidad todos los aspectos relacionados con el control de acceso, la seguridad en entornos inalámbricos y la formación de los usuarios en privacidad y seguridad. Las principales preguntas de investigación a las que queremos dar respuesta son:

- ¿Siguen los sistemas de historias clínicas electrónicas políticas de control de acceso? Se analizarán en profundidad todos los aspectos más relevantes que tengan que ver con las políticas de control de acceso que utilizan los actuales sistemas de historias clínicas electrónicas.
- ¿Quién realiza la gestión del acceso? Interesa conocer si es el paciente o el personal sanitario cualificado quien asigna y revoca el acceso a las historias clínicas electrónicas de los pacientes.
- ¿Se adoptan medidas de seguridad en entornos inalámbricos?
- ¿Es necesaria la formación de los usuarios del sistema de historias clínicas electrónicas?

Métodos

Revisión sistemática, protocolo y registro

Los autores usaron métodos formales en la revisión sistemática de la literatura para asegurar una búsqueda y un proceso de recuperación pertinentes y precisos. Para realizar la revisión se siguieron las recomendaciones del estándar PRISMA[4]. Por lo tanto, antes de iniciar la búsqueda en la literatura y la extracción de los datos posteriores se desarrolló un protocolo de revisión que describe cada paso de la revisión sistemática, incluidos los criterios de exclusión. Este protocolo fue revisado y aprobado por uno de los autores (Toval).

Criterios de inclusión

1) Fecha de publicación entre enero de 2006 y enero de 2011.
2) Artículos que versen sobre mecanismos de control de acceso, seguridad en entornos inalámbricos y formación de usuarios en temas de privacidad y seguridad, todo ello en el marco de sistemas de historias clínicas electrónicas.

Se incluyeron artículos publicados entre enero de 2006 y enero de 2011, 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[5] publicada en 2008 y actualizada en 2010. El segundo criterio de elegibilidad se incluye para poder responder a las preguntas de investigación planteadas.

Fuentes de información

La búsqueda se realizó en 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 en enero de 2011. Además de los artículos encontrados al consultar estas bases de datos, se revisaron las referencias de los artículos incluidos para que la revisión fuese más exhaustiva.

Selección de los estudios

La selección de los estudios se organizó en las siguientes cuatro etapas:

1) Búsqueda de publicaciones en las bases de datos electrónicas relacionadas con la salud y la informática. Para realizar la búsqueda se usó la siguiente cadena de búsqueda: (“electronic health record” AND (“accesscontrol” OR (“security” AND “wireless”) OR (“security” AND “privacy” AND “training”))), 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 encajaban o no en el estudio de acuerdo con los criterios de elegibilidad.
4) Se llevaron a cabo un seguimiento de citas y un 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 las realizaron dos autores de forma independiente. Cualquier discrepancia o duda se resolvió con la consulta a un tercer miembro del equipo. La selección se desarrolló en un proceso iterativo mediante evaluaciones individuales hasta que se alcanzó una fiabilidad interevaluador aceptable (0,83).

Proceso de recopilación de los datos

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

Análisis de los datos

Se diseñó una plantilla con los datos que debían extraerse de cada artículo. Estas características se agruparon en cinco categorías:

- Generales: autores, año de publicación, origen editorial, país de procedencia, resumen, aportaciones originales, principales hallazgos, conclusiones y otras aclaraciones.
- Respuesta a la primera pregunta: políticas de acceso, creación y concesión de control de acceso basado en roles (RBAC).
- Respuesta a la segunda pregunta: concesión de permisos por parte de pacientes, médicos o proveedores de la salud.
- Respuesta a la tercera pregunta: seguridad en entornos inalámbricos.
- Respuesta a la cuarta pregunta: formación de los usuarios del sistema en temas de seguridad y privacidad.

Resultados

Selección de los estudios

En total se incluyeron 24 artículos en la revisión. La búsqueda en las bases de datos proporcionó 1208 artículos, de los cuales se

Tabla 1
Resumen de los estudios incluidos en la revisión

Autores	Año	Título
Falcão-Reis et al.[6]	2008	Access and privacy rights using web security standards to increase patient empowerment
Röstad[7]	2008	An initial model and a discussion of access control in patient controlled health records
Daglish y Archer[8]	2009	Electronic personal health record systems: a brief review of privacy, security, and architectural issues
Kahn y Sheshadri[9]	2008	Medical record privacy and security in a digital environment
Benaloh et al.[10]	2009	Patient controlled encryption: ensuring privacy of electronic medical records
Farzandipour et al.[11]	2009	Security requirements and solutions in electronic health records: lessons Learned from a comparative study
Hu et al.[12]	2009	A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations
Win et al.[13]	2006	Personal health record systems and their security protection
Van der Linden et al.[14]	2009	Inter-organizational future proof EHR systems: a review of the security and privacy related issues
Lovis et al.[15]	2007	Comprehensive management of the access to the electronic patient record: towards trans-institutional networks
Riedl et al.[16]	2007	A secure architecture for the pseudonymization of medical data
Rostad y Edsberg[17]	2006	A study of access control requirements for healthcare systems based on audit trails from access logs
Choe y Yoo[18]	2008	Web-based secure access from multiple patient repositories
Agrawal y Johnson[19]	2007	Securing electronic health records without impeding the flow of information
Elger et al.[20]	2010	Strategies for health data exchange for secondary, crossinstitutional clinical research
Narayan et al.[21]	2010	Privacy preserving EHR system using attribute-based infrastructure
Hembroff y Muftic[22]	2010	SAMSON: secure access for medical smart cards over network
Zhang y Liu[23]	2010	Security models and requirements for healthcare application clouds
Sun y Fang[24]	2010	Cross-domain data sharing in distributed electronic health record systems
Al Faresi et al.[25]	2010	A comprehensive privacy-aware authorization framework founded on HIPAA privacy rules
Haas et al.[26]	2011	Aspects of privacy for electronic health records
Ardagna et al.[27]	2010	Access control for smarter healthcare using policy spaces
Jafari et al.[28]	2010	Using digital rights management for securing data in a medical research environment
Quantin et al.[29]	2011	Medical record search engines, using pseudonymised patient identity: an alternative to centralized medical records

descartaron 316 por no cumplir el primer criterio de inclusión. De los 892 que quedaban, 818 se descartaron tras revisar los títulos, resúmenes y palabras clave, por no cumplir el segundo criterio de inclusión. El texto de los 74 artículos restantes se examinó por completo. Se descartaron 57 por no cumplir el segundo criterio, lo que nos deja 17 artículos en la revisión. Adicionalmente, tras la revisión de las referencias de estos artículos se incluyeron 7 estudios más. La tabla 1 muestra un listado de todos los artículos incluidos en la revisión. En la figura 1 puede verse el diagrama de flujo del estándar PRISMA resumiendo estas etapas.

Características de los estudios

1) Políticas de acceso

Una política de control de acceso autoriza a determinados usuarios a realizar un conjunto de acciones en un conjunto de recursos, si se cumplen unas determinadas condiciones. Veintiún trabajos (87,5%) mencionan las políticas de acceso, de los cuales 13 (61,9%) usan para implementarlas el (RBAC)[6,7,9,14,15,17–20,23–25,28], que se convierte en el método de control de acceso por excelencia en muchos de los trabajos. Así, cada usuario que accede al sistema tiene asignado un rol, el cual tiene definidos una serie de permisos y restricciones. Uno de los trabajos mencionados añade una capa más de seguridad al requerir una autentificación mediante una tarjeta inteligente[15], otro obliga a acceder con un certificado digital[18], otro añade un *proxy* de firmas digitales para conseguir un control de acceso de grano fino[24] y otro utiliza la gestión de derechos digitales para controlar el acceso a las historias clínicas electrónicas usando licencias[28]. Algunos otros métodos de acceso ofrecidos en los estudios son mediante usuario/contraseña[10,13,21], certificado válido de seguridad de una organización de confianza[8], con una tarjeta inteligente con número de identificación personal (PIN)[13,16], con una tarjeta inteligente con PIN más la huella digital del paciente[22] y mediante conjuntos/espacios de políticas de acceso[27]. En cuanto a la forma de creación del RBAC, 10 (47,62%) artículos hablan de qué personas u organismos definen los roles y qué roles son creados en un sistema de historias clínicas electrónicas[6–9,14,15,18,23,24,28]. De ellos, 7 (70%) proponen que los roles sean definidos previamente por instituciones, hospitales o algún comité institucional[8,9,14,15,18,23,24], aunque tres[8,14,15] plantean que el paciente pueda incluir refinamientos o restricciones, de manera que permitan personalizarlos. Röstad[7] presenta un modelo en el cual parte de los roles son creados por el sistema, definidos inicialmente, y otros puede definirlos el usuario. Además, cinco de los artículos incluidos[6,17,22,26,27] indican que en situaciones de emergencia, si la vida del paciente puede encontrarse en peligro, será necesario saltarse las políticas de acceso definidas.

2) Administración de los permisos

Diecinueve trabajos (79,17%) tratan la concesión de los permisos de acceso a las historias clínicas electrónicas[6–8,10,12,14–16,18–28]. De ellos, 14 indican que es el paciente quien concede los permisos[6,7,10,12,16,18–22,25–28]. Narayan et al.[21] proponen que los profesionales sanitarios pueden delegar el acceso a otros profesionales sanitarios, una vez obtenido el permiso del paciente, y Al Faresi et al.[25] indican la existencia de guardianes de las historias clínicas electrónicas (personal médico o de enfermería, etc.) que realizan una microgestión de ellas y deciden si se pueden aplicar las preferencias del paciente basándose en el cumplimiento de la ley de portabilidad y responsabilidad del seguro médico (HIPAA, *Health Insurance Portability and Accountability Act*). Tres de los trabajos[15,23,24] indican que el servicio médico es el que da el permiso de acceso, uno señala que tanto el paciente como la administración asignan normas para la disponibilidad de los datos del paciente[8], y otro dice que pueden elegirse dos enfoques:[14] el consentimiento implícito, en el cual el paciente asume que consiente las reglas predefinidas a menos que indique lo contrario, y el consentimiento explícito, por el cual prohíbe el acceso a la información a menos que dé su consentimiento.

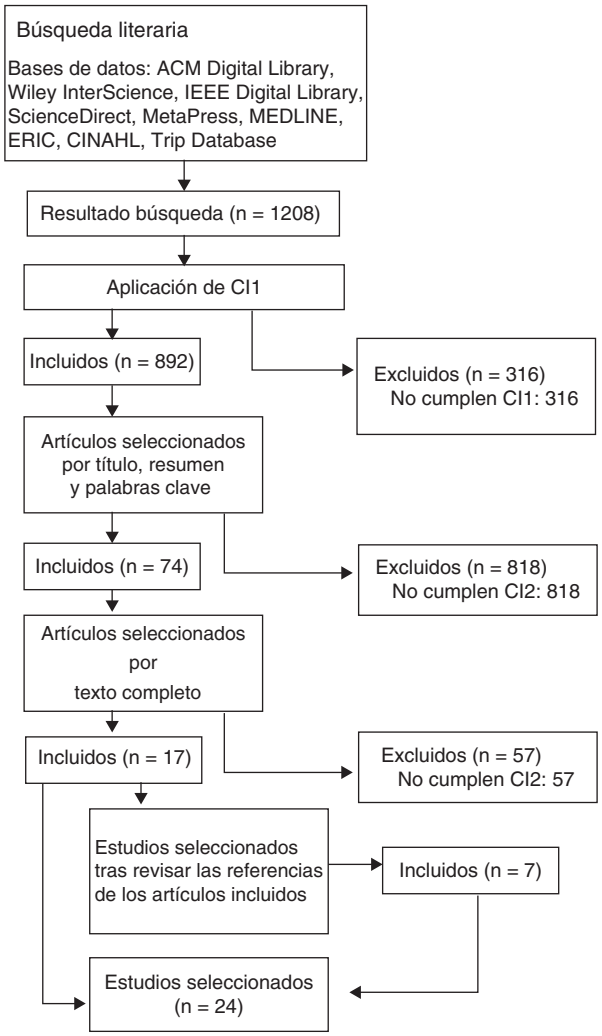

Figura 1. Diagrama de flujo de PRISMA.

3) Dispositivos inalámbricos

Únicamente tres artículos (20%)[8,9,13] abordan la seguridad en entornos inalámbricos. Daglish y Archer[8] proponen mecanismos de seguridad a la hora de realizar una implantación en las historias clínicas electrónicas. Identifican[9] el problema de mantener la privacidad y la seguridad en los entornos médicos inalámbricos y dan algunas soluciones para mejorarlas en los sistemas de historias clínicas electrónicas. Otros tres artículos[23,26,29] proponen que las comunicaciones en general sean seguras mediante el envío de datos cifrados y el uso de SSL, TSL o IPSec, pero no especifican si esas comunicaciones se realizarán en entornos inalámbricos.

4) Formación

En los trabajos revisados no se menciona excesivamente si es necesaria la formación del personal: cuatro trabajos (26,6%) indican que sí es necesaria[6,9,11,20]. La mitad de los trabajos sólo señalan que es necesaria la formación del personal sanitario[9,11], mientras que Falcao-Reis et al.[6] dicen que es necesaria la formación de los usuarios en general, tanto profesionales de la salud como de los pacientes.

Discusión

¿Siguen los sistemas de historias clínicas electrónicas políticas de control de acceso?

La característica más importante extraída de la revisión es la utilización de políticas que definen el acceso a los datos del paciente. Algunos trabajos[6,17,22,26,27] proponen que debe haber un mecanismo que se salte las políticas de acceso en situaciones de emergencia, cuando la vida del paciente podría estar en peligro. El control de acceso preferido es el basado en roles (RBAC). Sin embargo, algunos autores critican que este método no permite una compartición selectiva de los datos de grano fino, y lo combinan con otros métodos como la autenticación con tarjeta inteligente[15], el certificado digital[18] y un *proxy* de firmas digitales[24]. En cuanto a la forma de creación del RBAC, se observa que los autores se pronuncian mayoritariamente por roles creados por las organizaciones, pues detectan que si los roles de acceso a una historia clínica electrónica pudiese crearlos un usuario, dificultaría extremadamente el sistema de historias clínicas electrónicas, así como la interoperabilidad con otros sistemas de historias clínicas electrónicas.

¿Quién realiza la gestión del acceso?

En cuanto a la administración de los permisos de acceso a las historias clínicas electrónicas, se observa que en los últimos años se está imponiendo de manera inevitable que los pacientes sean los propietarios de sus propias historias clínicas electrónicas y, por tanto, que sean ellos quienes deciden quién puede ver su información sanitaria y cuándo. Esta opinión se ve favorecida gracias a que se están planteando sistemas Web que permiten al paciente acceder a su historia clínica electrónica, consultarla, modificarla y observar quién ha accedido a ella, en qué momento y con qué propósito. Ahora mismo, compañías importantes como Microsoft[30] han lanzado sistemas web donde el paciente tiene control sobre sus datos. Estos sistemas se denominan «historias personales de salud» y mejoran la comunicación médico-paciente, y aunque podrían no tener cabida en un sistema sanitario como el español, sí podrían utilizarse la experiencia y los datos de las historias personales de salud para mejorar los sistemas de historias clínicas electrónicas, cuando el paciente tenga un mayor protagonismo en sumanejo.

¿Se adoptan medidas de seguridad en entornos inalámbricos?

Se ha detectado que muy pocos trabajos mencionan los dispositivos inalámbricos, cuando es un aspecto considerado de gran importancia puesto que las comunicaciones son cada día más móviles, y permitir tanto al paciente como al personal médico acceder a la información a través de medios inalámbricos puede suponer un gran problema de seguridad si la red no está lo suficientemente protegida. La adopción de los dispositivos móviles en la atención sanitaria es una realidad. Las nuevas tecnologías pueden hacer posible el seguimiento, las consultas y la asistencia médica a distancia, consiguiendo que estos servicios sean más flexibles y convenientes, ya que proporcionan al facultativo mayor información sobre el paciente y con más rapidez[31,32].

¿Es necesaria la formación de los usuarios del sistema de historias clínicas electrónicas?

Se considera que, dada la criticidad de los aspectos de seguridad y privacidad en los sistemas de historias clínicas electrónicas, resulta necesario que tanto el personal sanitario como los pacientes reciban una correcta formación en temas de seguridad para intentar evitar en lo posible exponer información sensible. Sin embargo, sólo cuatro trabajos mencionan este aspecto. La mitad de ellos

indican que debe formarse al personal sanitario, y sólo uno incluye a los usuarios del sistema en general.

Un sistema de historias clínicas electrónicas con un control de acceso basado en roles, al cual se acceda mediante un certificado de seguridad o una tarjeta inteligente, parece una opción prometedora para proteger las historias clínicas electrónicas de intrusos, según los estudios analizados. Se ha observado una característica a la cual apenas se hace mención, y es la seguridad en los entornos inalámbricos. Dada la sensibilidad de la información sanitaria y la naturaleza de los entornos inalámbricos, que presentan sus propias amenazas de seguridad, debería prestarse especial atención a los protocolos utilizados (WEP, WPA y WPA2) y a los posibles ataques de seguridad publicados cada día en bases de datos de vulnerabilidades como OSVDB y NIST. Además, los sistemas de historias clínicas electrónicas pueden seguir diferentes estándares para mejorar y, de alguna forma, garantizar la seguridad y la privacidad de los datos. En cuanto al control del acceso, nosotros recomendamos seguir el estándar ISO 13606[5], que define un marco básico que puede utilizarse como una especificación mínima de políticas de control de acceso a las historias clínicas electrónicas[17].

¿Qué se sabe sobre el tema?

La seguridad y la privacidad son muy importantes en cualquier sistema informático, pero en los de historias clínicas electrónicas son cruciales. Estos sistemas tienen poca interoperabilidad.

¿Qué añade el estudio realizado a la literatura?

El mecanismo de control de acceso más utilizado es el basado en roles: el usuario o el profesional médico son los que gestionan el control de acceso. La seguridad en entornos inalámbricos está poco estudiada. El control de acceso basado en roles no permite un control de grano fino, por lo que habría que diseñar un sistema que lo haga posible. Dada la importancia que están cobrando los entornos inalámbricos en los sistemas de historias clínicas electrónicas, los desarrolladores deben implementar sistemas de seguridad adaptados a la naturaleza de estos sistemas.

Contribuciones de autoría

I. Carrión Señor buscó publicaciones indexadas en bases de datos relacionadas con las ciencias de la salud y la computación; revisó el resultado de la búsqueda, explorando el título, el resumen y las palabras clave de los artículos identificados; seleccionó los artículos incluidos en la revisión, basándose en los criterios de elegibilidad definidos; leyó el texto completo de los artículos que no se habían descartado aún, para determinar si se incluían o no en la revisión, siempre de acuerdo con los criterios de elegibilidad definidos; revisó la lista de referencias de los artículos ya seleccionados para descubrir nuevos estudios que pudieran tener cabida en este estudio; evaluó los artículos potencialmente relevantes para extraer sus características principales y comprobó las extraídas de otros artículos realizadas por otro autor; finalmente, escribió parte del artículo que explica esta investigación. J.L. Fernández Alemán desarrolló el protocolo de revisión que describe cada paso de esta revisión sistemática, incluyendo los criterios de elegibilidad; buscó publicaciones en bases de datos electrónicas relacionadas con las ciencias de la salud y la computación; revisó el resultado de esta búsqueda, explorando el título, el resumen y las palabras clave, y los seleccionó según los criterios de elegibilidad definidos; leyó el texto completo de los artículos que no habían sido previamente descartados para determinar si deberían ser incluidos en la revisión; evaluó la lista de referencias de artículos seleccionados para descubrir nuevos estudios, que fueron revisados; evaluó los artículos potencialmente relevantes para este estudio, para extraer sus características principales, y comprobó las extraídas de los artículos por otros autores; finalmente, revisó y escribió parte de este artículo que explica la investigación realizada. A. Toval revisó y aprobó el protocolo usado para realizar la revisión sistemática; resolvió discrepancias entre el resto de los autores durante la fase de selección de los estudios; y revisó este artículo que explica el estudio realizado.

Financiación

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia e Innovación, proyecto PEGASO, TIN2009-13718-C02-01, PANGEA, TIN2009-13718-C02-02.

Conflictos de intereses

Ninguno.

Bibliografía

1. Hesse BW, Hansen D, Finholt T, et al. Social participation in health 2.0. Computer. 2010;43:45–52.
2. Carnicero J. Desarrollo de la eSalud en Europa. 2011. Disponible en: http://www.cepal.org/dds/noticias/paginas/2/41012/salude-Europa-Javier-Carnicero.pdf
3. Carrión Señor I, Fernández Alemán JL, Toval A, et al. Seguridad y privacidad en historiales clínicos electrónicos: una revisión sistemática de la literatura. Revista eSalud com. 2011;7:1–11.
4. Liberati A, Altman DG, Tetzlaff J, et al. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. J Clin Epidemiol. 2009;62:e1–34.
5. Norma ISO/CEN 13606 [Internet]. (Actualizado el 1/8/2011; consultado el 20/7/2011.) Disponible en: www.aenor.es.
6. Falcao-Reis F, Costa-Pereira A, Correia ME. Access and privacy rights using web security standards to increase patient empowerment. Stud Health Technol Inform. 2008;137:275–85.
7. Röstad L. An initial model and a discussion of access control in patient controlled health records. En: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. Washington, DC: IEEE Computer Society; 2008. p. 935-42.
8. Daglish D, Archer N. Electronic personal health record systems: a brief review of privacy, security, and architectural issues. En: Proceedings of the 2009 World Congress on Privacy, Security, Trust and the Management of e-Business. Washington, DC: IEEE Computer Society; 2009. p. 110–20.
9. Kahn S, Sheshadri V. Medical record privacy and security in a digital environment. IT Professional. 2008;10:46–52.
10. Benaloh J, Chase M, Horvitz E, et al. Patient controlled encryption: ensuring privacy of electronic medical records. En: Proceedings of the 2009 ACM Workshop on Cloud Computing Security. New York: ACM; 2009. p. 103–14.
11. Farzandipour M, Sadoughi F, Ahmadi M, et al. Security requirements and solutions in electronic health records: lessons learned from a comparative study. J Med Syst. 2009;34:629–42.
12. Hu J, Chen HH, Hou TW. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards & Interfaces. 2010;32:274–80.
13. Win KT, Susilo W, Mu Y. Personal health record systems and their security protection. J Med Syst. 2006;30:309–15.
14. van der Linden H, Kalra D, Hasman A, et al. Inter-organizational future proof EHR systems: a review of the security and privacy related issues. Int J Med Inform. 2009;78:141–60.
15. Lovis C, Spahni S, Cassoni N, et al. Comprehensive management of the access to the electronic patient record: towards trans-institutional networks. Int J Med Inform. 2007;76:466–70.
16. Riedl B, Neubauer T, Goluch G, et al. A secure architecture for the pseudonymization of medical data. En: Proceedings of the The Second International Conference on Availability, Reliability and Security. Washington, DC: IEEE Computer Society; 2007. p. 318–24.
17. Rostad L, Edsberg O. A study of access control requirements for healthcare systems based on audit trails from access logs. En: Proceedings of the 22nd Annual Computer Security Applications Conference. Washington, DC: IEEE Computer Society; 2006. p. 175–86.
18. Choe J, Yoo SK. Web-based secure access from multiple patient repositories. Int J Med Inform. 2008;77:242–8.
19. Agrawal R, Johnson C. Securing electronic health records without impeding the flow of information. Int J Med Inform. 2007;76:471–9.

20. Elger BS, Iavindrasana J, Lo Iacono L, et al. Strategies for health data exchange for secondary, cross-institutional clinical research. Comput Methods Programs Biomed. 2010;99:230–51.
21. Narayan S, Gagné M, Safavi-Naini R. Privacy preserving EHR system using attribute-based infrastructure. En: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop. New York: ACM; 2010. p. 47–52.
22. Hembroff GC, Muftic S. SAMSON: Secure Access for Medical Smartcards Over Networks. En: Proceedings of the 2010 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). Washington, DC: IEEE Computer Society; 2010. p. 1-6.
23. Zhang R, Liu L. Security models and requirements for healthcare application clouds. En: Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing. Washington, DC: IEEE Computer Society; 2010. p. 268-75.
24. Sun J, Fang Y. Cross-domain data sharing in distributed electronic health record systems. IEEE Transactions on Parallel and Distributed Systems. 2010;21:754–64.
25. Al Faresi A, Wijesekera D, Moidu K. A comprehensive privacy-aware authorization framework founded on HIPAA privacy rules. En: Proceedings of the 1st ACM International Health Informatics Symposium. NewYork: ACM; 2010. p. 637-46.
26. Haas S, Wohlgemuth S, Echizen I, et al. Aspects of privacy for electronic health records. Int J Med Inform. 2011;80:e26–31.
27. Ardagna CA, di Vimercati SDC, Foresti S, et al. Access control for smarter healthcare using policy spaces. Computers & Security. 2010;29: 848–58.
28. Jafari M, Safavi-Naini R, Saunders C, et al. Using digital rights management for securing data in a medical research environment. En: Proceedings of the 10th Annual ACM Workshop on Digital Rights Management. New York: ACM; 2010. p. 55-60.
29. Quantin C, Jaquet-Chiffelle DO, Coatrieux G, et al. Medical record search engines, using pseudonymised patient identity: an alternative to centralized medical records. Int J Med Inform. 2011;80:e6–11.
30. Microsoft. Microsoft HealthVault. 2007. Disponible en: www.microsoft.com/en-us/healthvault/.
31. Tachakra S, Wang XH, Istepanian RS, et al. Mobile e-health: the unwired evolution of telemedicine. Telemed J E Health. 2003;9:247–57.
32. Kyriacou EC, Pattichis CS, Pattichis MS. An overview of recent healthcare support systems for eEmergency and mHealth applications. En: Conf Proc IEEE. Eng Med Biol Soc. 2009:1246–9.