Curso de Introducción a la Historia Clínica Electrónica

Seguridad, Privacidad y Confidencialidad

Material elaborado por equipo docente - 2017

Tabla de contenido

Seguridad, Privacidad y Confidencialidad

Esta sección estará dedicada al Componente de Seguridad. Comenzaremos primero definiendo los conceptos de **privacidad, confidencialidad y seguridad** de la información en salud. Para garantizar cierta comprensión integral del problema, **ejemplificaremos** con varios casos reportados en la literatura mundial, haciendo hincapié también en las **medidas regulatorias** que fueron implementadas a lo largo del planeta, que intentan proteger esta información.

Daremos lugar a una breve revisión de las diferentes estrategias para la protección de la información electrónica en salud, como ser la gestión de usuarios y accesos a los diferentes aplicativos del sistema; para luego concluir con una introducción y puesta al día de la herramienta que actualmente permite garantizar la autoría y la integridad de los registros electrónicos: **la Firma Electrónica/Digital en Salud**.

Definiciones

Algunos de los desafíos más significativos con los que se enfrentan los Sistemas de Información en Salud están relacionados con garantizar el acceso a la información y la protección de la privacidad y confidencialidad. La seguridad tiene una estrecha relación con estos dos conceptos, por lo que resulta indispensable definirlos, ya que en este escenario tienen significados muy específicos. Distintos autores pueden usarlos de diferentes maneras, acordemos las siguientes definiciones para este curso:

Privacidad es el derecho a quedarse con información para uno mismo.

Confidencialidad es el derecho de que la información comunicada a alguien (en confidencia) no sea transmitida a terceros.

Seguridad consiste en los medios utilizados para garantizar la confidencialidad y evitar la vulneración de la privacidad y la pérdida de información. En otras palabras, la seguridad de la información consiste en procesos y controles diseñados para proteger información de su divulgación no autorizada, transferencia, modificación o destrucción, a los efectos de:

- Asegurar la continuidad
- Minimizar posibles daños
- Maximizar oportunidades

Descripción del problema

La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada. La información puede estar impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o medios electrónicos, microfilmada, hablada en conversación o grabada. Tan sólo las computadoras son capaces de manejar la inmensa cantidad de información clínica generada en una institución, pero son los profesionales de la salud quienes necesitan acceso a esta información a la hora de tomar decisiones. El problema surge a la hora de hacerla disponible: se crean oportunidades para que individuos ajenos al cuidado de la salud de un paciente, tengan acceso a su información médica. En el mejor de los casos, se trata de empleados curiosos de la misma institución. Pero podrían existir personas que (dentro y fuera de la institución) buscan sacar algún beneficio con la información obtenida, o usarla de alguna forma en contra del paciente cuya privacidad fue violada, o la misma institución.

Los responsables de esta información clínica se encuentran en una encrucijada, en la que deben decidir entre mejorar la calidad de atención con sistemas informáticos (permitiendo acceder a esta información), o proteger la privacidad y la confidencialidad de

sus pacientes, restringiendo el uso de los sistemas. Por suerte, estos dos objetivos no son incompatibles.

Esta problemática fue ampliamente descripta en la literatura (1–5), y a continuación vamos a repasar algunos casos representativos.

Rindfleisch en un trabajo realizado en 1997 (6) agrupó las problemáticas que acarrea la difusión de información relacionada con la salud en problemas de:

- discriminación, cuando el paciente puede ser objeto de discriminación por conocerse que sufre una enfermedad determinada, como el HIV; o por tener una predisposición para desarrollar cierta patología, como factores de riesgo genéticos para cáncer de mama.
- marketing, cuando sea el blanco de estrategias de marketing orientadas a su enfermedad o riesgo.

Existen también casos de **difusión no intencional de información en salud.** Un trabajo publicado en 2003 demostró que, utilizando Google, es posible acceder a información de pacientes y detectar puntos de acceso a bases de datos no seguras (7). Otro trabajo del mismo autor reportó que en 2003 un hacker entró en una base de datos de 7,000 pacientes de una clínica de desórdenes del sueño en Indiana (8). Otro casi conocido en el ámbito de la salud es del año 2001 en la Universidad de Washington, cuando un hacker entró en la base de datos de cardiología y obtuvo acceso a información de más de 5,000 pacientes (9).

Opinión Pública

Ante estos eventos, parte del público está preocupada por los **riesgos del almacenamiento electrónico de información sensible**. La privacidad y la confidencialidad de la información son derechos de las personas (10,11), y no es necesario dar una razón

para que la información sensible sea un dato protegido. Una encuesta realizada en el año 2005 en los Estados Unidos, conducida por Harris Interactive, encontró que la opinión pública está dividida sobre si el beneficio supera los riesgos o no para la utilización de un registro médico electrónico: el 47% estuvo a favor y el 48% en contra. También se encontró que el 82% de los encuestados querrían disponer de herramientas para rastrear su propia información en salud y asegurar su derecho a la privacidad (12).

Podríamos decir entonces que garantizar la privacidad y la confidencialidad beneficia también al Sistema de Salud, ya que un paciente que sabe que su información clínica no será accedida de forma inapropiada, se sentirá más cómodo a la hora de revelarla; y lograr esta confianza es vital para mantener la relación médico-paciente o enfermero-paciente.

El riesgo para la privacidad de la información

Una estrategia muy utilizada para intercambiar información es compartir los datos médicos con fines estadísticos y de gestión, pero sin brindar los datos completos de las personas, lo que comúnmente se denomina desidentificación de la información. Esta forma "no-identificada" por ejemplo, ofrecería los diagnósticos con:

- El código postal
- El sexo
- La fecha de nacimiento

Sweeney revisó esta estrategia en 2002, y concluyó que el 87% de la población de EE.UU. se puede identificar con el código postal, el sexo y la fecha de nacimiento. Identificaron, como ejemplo, al gobernador de Massachusetts, al cruzar los datos "no-identificados" del seguro de salud público con un padrón electoral (13).

La información médica tiene muchos usos más allá del asistencial, Rindfleisch (Figura 1) agrupó estos usos en:

- Actividades de soporte a la atención médica.
- Usos sociales.
- Usos comerciales.

Esto provoca que, aunque una institución cuide con mucho detalle la información que recolecta, la misma viaja por muchos canales y a diferentes destinatarios donde se corre el riesgo de que comprometa la privacidad de los pacientes (6).

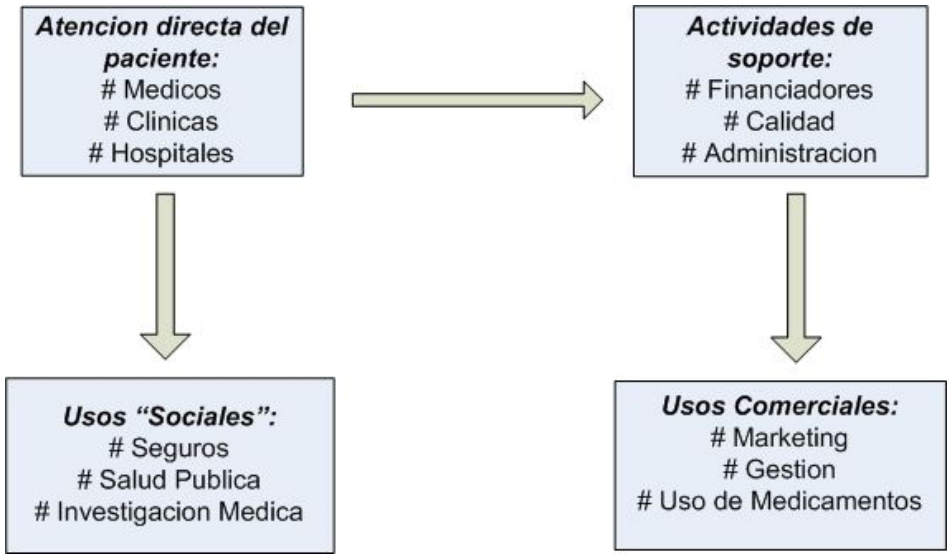

Figura 1: Flujo de Datos de Rindfleisch (Adaptado, 1997)

El riesgo para la privacidad de la información no es algo relacionado con los registros electrónicos; ya el **registro en papel** tiene muchas debilidades en este aspecto. Es muy difícil rastrear quién vio un registro en papel o en qué sectores de la institución fue utilizado. Con una simple fotocopiadora, cámara de fotos o máquina de fax es posible

llevarse información privada. Esto permite que la copia de registros en papel sea una práctica común, siendo requisito ante mudanzas, cambios de equipo de atención, cambios de cobertura de salud, pólizas de seguro, etc.

Podemos concluir que, aunque los registros informáticos tengan algunos riesgos, con el papel se corren aún mayores riesgos. La posibilidad de los registros informáticos de registrar todos los accesos y las copias de resguardo le dan a una seguridad mayor que el papel.

La falta de seguridad en los registros de salud puede traer diversas consecuencias:

- Los pacientes reaccionan evitando consultar en determinados casos, o mienten durante las consultas con los riesgos que esto acarrea para su tratamiento.
- Los médicos no registran información sensible, aunque pueda ser de valor clínico en el futuro para ellos mismos o sus colegas. Los médicos inventan formas de registrar información adicional fuera del registro oficial, quitándole su función de herramienta de comunicación entre el equipo de salud.
- Mientras tanto, la falta de seguridad hace que eventualmente aparezcan nuevos casos de difusión de información privada.

Estrategias de Protección de Seguridad

Pese a la gran cantidad de evidencia existente sobre esta problemática, existen aún varios temas relacionados con los registros médicos que todavía permiten cierta discusión, o por lo menos, llaman a la reflexión: ***¿Quién es el propietario de la información médica?***

Clásicamente el propietario era la institución o el médico que registraba la información. Actualmente hay una tendencia internacional a proponer que el propietario de la información sea el paciente y, por lo tanto, éste debería tener libre acceso a la misma y a restringir su uso de acuerdo con sus necesidades. En muchos países existe legislación

vigente que establece que la información médica es propiedad de las personas, como la ley 26529 en Argentina (14). Cabe preguntarse entonces: ***¿Cuáles son los límites del derecho a la privacidad?*** Entre otros:

- Motivos de salud pública
- El derecho a investigar
- La evidencia de delitos contenida en el registro médico

Por último, es necesario explorar los posibles conflictos comerciales que puede presentar la utilización de la información registrada. Uno de los primeros trabajos orientados a responder esta pregunta fue el reporte del Institute of Medicine (IOM), llamado "The computer based patient record", inicialmente editado en 1991 y revisado en 1997. Este informe fue comisionado por la Biblioteca Nacional de Medicina de EE.UU (National Library of Medicine - NLM), y revisó la forma de trabajo de seis instituciones. El reporte recomienda diferentes estrategias para proteger la información en salud en sistemas informáticos (15). Aunque algunos puntos pueden estar desactualizados, la estructura general está completamente vigente. El reporte define los lugares desde donde pueden surgir las amenazas a la seguridad de la información, dividiéndolas principalmente en internas y externas.

Las más importantes son las **internas,** que incluyen:

- La revelación accidental de datos
- La curiosidad del personal
- La posibilidad de sobornos para la entrega de información personal

Cuando se envía información para uso secundario, como facturación, epidemiología, y otros, puede haber también exposiciones de información personal. Las causas **externas,** como el ingreso de hackers o piratas informáticos, ha sido muy publicitada pero, en la realidad, hay muy pocos ejemplos de ellas. El reporte propone adoptar algunas de las

siguientes **medidas de seguridad**, relacionadas con la organización estructural de la institución:

- Establecer políticas claras y comités sobre seguridad y confidencialidad.
- Implementar Programas de Educación y Entrenamiento.
- Aplicar sanciones claras al personal que viola las normas de seguridad y confidencialidad
- Facilitar el acceso de los pacientes a las auditorías de recorrido.

El mismo reporte delinea algunas:

- Autenticación de los usuarios.
- Registro detallado de accesos.
- Seguridad física de los datos.
- Protección en los puntos de acceso remoto y comunicaciones externas.
- Método estricto de desarrollo del Software.
- Control permanente de vulnerabilidades.

Tecnologías para asegurar la información

Para afianzar la seguridad de la información se implementan **diferentes estrategias.** Algunas apuntan a vigilar el manejo de información, haciendo que los usuarios se cuiden del uso que hacen de ella. Ejemplos de eso son las alertas en el momento de visualizar información sensible y el registro detallado de todo contacto de los usuarios con la información, las llamadas “Auditorias de recorrido” o “Trail audits”. Otras apuntan a mejorar la administración de sistemas, contar con normas para el manejo el software y la asignación y el control de accesos, o la realización de análisis de vulnerabilidad de los sistemas. La estrategia más utilizada para asegurar la información es la utilización del clásico

par "**usuario y contraseña**". Esta herramienta puede incluir diferentes niveles de complejidad como veremos a continuación.

Validación de identidad mediante "usuario y contraseña"

Un área importante en la seguridad de la información es la autenticación de usuarios y contraseñas para ingresar a los sistemas.

Los factores humanos de autenticación se clasifican en:

- Algo que el usuario posea (por ejemplo: tarjeta, token de seguridad, teléfono).
- Algo que el usuario sepa (por ejemplo: nombre de usuario, contraseña, frase clave, PIN).
- Algo que sea característico del usuario (por ejemplo: huella digital, lectura retina, secuencia ADN, reconocimiento firma o de la voz).

Comencemos definiendo algunos conceptos:

Autenticación: es el acto de establecer o confirmar que una cosa (o persona) es auténtica, es decir que lo que se desea aseverar es verdad. La autenticación de una persona consiste en verificar su identidad.

Autorización: proceso de verificar que una persona conocida tiene la autorización para realizar una tarea u operación. Por lo tanto, la autenticación precede la autorización.

Identificación Uni-Factor: es la modalidad de identificación más utilizada en internet y en Salud, para la cual un usuario se identifica en el sistema ingresando nombre de usuario y contraseña (utiliza sólo el factor: algo que el usuario sabe).

La identificación Uni-Factor se basa en el concepto "algo que uno sabe". No obstante esta forma de identificación es la más vulnerable dentro de los sistemas dado que cualquier persona que sepa nombre de usuario y contraseña puede ingresar. Además la gestión de las

contraseñas en el entorno de la Salud suele ser un problema. Para aumentar aún más la seguridad de un Sistema es necesario sumar a la contraseña algún dispositivo físico (algo que el usuario posea) o algo que sea característico del usuario (como la huella digital). Este tipo de estrategias combinadas se conoce como autenticación multi-factor y está actualmente en amplio desarrollo en muchos sistemas que requieren alta seguridad (bancos, tiendas comerciales.). El uso de dispositivos biométricos tal vez sea útil, pero en organizaciones a gran escala el costo de implementación puede ser muy alto. También se podría utilizar algún otro dispositivo como una tarjeta inteligente o "llavero" USB.

La Identificación Multi-Factor es un fuerte refuerzo a la autenticación. Se basa en utilizar 2 o más factores para la autenticación. Las formas más utilizadas de autenticación multi-factor son:

- Tarjeta + PIN, es el ejemplo del cajero automático (2 factores: algo que el usuario posea más algo que el usuario sepa).
- Contraseña + huella digital (2 factores: algo que el usuario sabe más algo que es característico del usuario).

Además de las estrategias para aumentar la seguridad, existen los obstáculos que también la resguardan.

Barreras implementadas para garantizar el correcto uso de la información

Un ejemplo es el requerimiento de autenticación para interactuar con el sistema: los usuarios se identifican con clave y contraseña para el acceso. Algunos centros requieren autorización explícita a cada médico para acceder a cada registro médico. Las firmas digitales son una forma de identificación del responsable de las acciones en el sistema en una manera más segura y, en algunos casos, tiene hasta validez legal, como vamos a ver

más adelante. La encriptación de los datos, requiriendo claves privadas de desencriptación, asegura que, aunque se pierdan datos, éstos no puedan ser utilizados. La correcta configuración de todas las herramientas de protección de redes, como los Firewalls, mejora la seguridad a las amenazas externas separando las redes institucionales de Internet.

La **encriptación** es una de las tecnologías más utilizadas para la seguridad de la información. Implementar la encriptación por sí sola no alcanza como medida de seguridad, pero su uso está altamente recomendado cuando se transmiten datos por redes públicas, como Internet.

El proceso de encriptación consiste en transformar la información en un texto incomprensible, que luego puede volver a su forma original. Para los dos procesos se requiere una clave. Un tipo de encriptación, la asimétrica de clave pública, es la base de la firma digital, un tema del que hablaremos más adelante.

Balance entre seguridad total y afectación del trabajo diario

Sigue siendo difícil definir **qué nivel de seguridad vamos a necesitar para la información en salud**. En ambos extremos del espectro están desde simples sitios Web completamente inseguros hasta organizaciones gubernamentales, militares o de inteligencia en las que la protección de la información es algo vital. Los sitios altamente seguros implementan una gran cantidad de medidas, como:

- Controles en el acceso.
- Prohibición de la utilización de medios portátiles como discos ópticos (CD, DVD), pendrives o computadoras portátiles.
- Control con cámaras de seguridad.
- Cambios obligatorios de contraseña periódicos.

Todas estas medidas son efectivas pero producen muchas molestias para los trabajadores y visitantes de estos centros, y su implementación en una institución de salud es muy discutible. El secreto es encontrar el punto ideal entre el costo y el beneficio de las medidas de control de seguridad de información electrónica en el ámbito de la salud.

Log-in Único

Al hablar de estándares, más específicamente, estándares de aplicaciones, mencionamos la necesidad de cierta interoperabilidad en las aplicaciones. Dentro de estos estándares, se incluyen algunos ejemplos que determinan cierta uniformidad en la visualización de la información y la interacción de los usuarios con las distintas aplicaciones, incluyendo la validación de identidad.

El log-in único es un proceso que permite a los usuarios de múltiples aplicaciones dentro del mismo sistema o entorno, utilizar un mismo nombre de usuario y contraseña, o en el caso de sistemas más avanzados, una única forma de validar su identidad (en el caso de la identificación multifactor). De esta forma, todos los datos necesarios para autenticar e identificar a un usuario se administran de forma independiente a las aplicaciones, y estas se alimentan de este repositorio único de usuarios. Una iniciativa dentro de la familia de estándares de HL7, es el Clinical Context Object Workgroup (CCOW), que intenta aplicar el single sign-on y la gestión contextual, combinándolos. Otra iniciativa de log-in único que está comenzando a tomar fuerza a nivel mundial es OpenID, un sistema de identificación digital descentralizado, en el que los usuarios puede identificarse en una página web que utilice el sistema. En este caso, los usuarios no tienen que crearse una nueva cuenta (nombre de usuario y contraseña) para obtener acceso, sino que necesitan disponer de un identificador creado por OpenID, mediante sitios llamados “proveedores de identidad”. La seguridad de una conexión OpenID depende de la confianza que tenga el cliente OpenID en el proveedor de identidad.

Gestión de Usuarios y Control de Accesos

Siguiendo las recomendaciones del IOM, y las experiencias recopiladas de la literatura, el Hospital Italiano de Buenos Aires (HIBA), creó un área de Gestión y Auditoría de Tablas Maestras. Como su nombre lo indica, mantienen actualizadas las tablas maestras, encargándose también de la gestión de usuarios y los accesos. De esta forma cada vez que una persona pasa a formar parte de la institución, le asignan los atributos necesarios (Profesión, Área, Especialidad, etc.), adquiriendo en ese mismo momento el acceso a los diferentes aplicativos (en algunos casos, se trata de accesos limitados hasta que cumplan cierta capacitación en el uso de los aplicativos) y el nivel de acceso que tendrá en los mismos. Por ejemplo:

- Un médico ingresa para desempeñarse como Médico Interno de Clínica Médica en la Internación. Su función dentro del ROL asistencial, será la de médico de guardia. Adquiere acceso completo a la historia clínica de todos los pacientes internados, en la sala general. No podrá consultar información de pacientes pediátricos ni pacientes dentro del MPI que no estén internados.
- Un enfermero que ingresa para desempeñarse como enfermero de un determinado sector de la internación. Su función dentro del ROL asistencial será la de enfermero. Esto le permite acceso restringido a los pacientes que tenga a su cargo en su sector de internación, o aquellos que le serán derivados de forma inmediata. No podrá ver información de pacientes internados fuera de su sector, ni pacientes no internados. Pero también tendrá acceso al sistema de ADT (admisión y egreso de pacientes).
- Una mujer que ingresa para desempeñarse como mucama de la internación. No tendrá ROL asistencial, pero si ROL institucional. Su función será mucama. No adquiere acceso a la historia clínica, ni ningún dato de ningún paciente del hospital. Si accede al sistema de ADT para indicar el momento en el que una cama está preparada para recibir otro paciente.

- Para el acceso al sistema fuera de la red institucional, se implementó una doble validación de identidad a través de la utilización de una tarjeta chip (qué es utilizada para la firma electrónica/digital de documentos médicos).

Referencias

1. Wynia MK, Torres GW, Lemieux J. Many physicians are willing to use patients' electronic personal health records, but doctors differ by location, gender, and practice. Heal Aff [Internet]. 2011/02/04. 2011;30(2):266–73. Available from: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=21289348

2. Malin B, Airoldi E. Confidentiality preserving audits of electronic medical record access. Stud Heal Technol Inf [Internet]. 2007/10/04. 2007;129(Pt 1):320–4. Available from: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=17911731

3. Malin B, Nyemba S, Paulett J. Learning relational policies from electronic health record access logs. J Biomed Inf [Internet]. 2011/02/01. 2011;44(2):333–42. Available from: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=21277996

4. Lovis C, Spahni S, Cassoni N, Geissbuhler A. Comprehensive management of the access to the electronic patient record: towards trans-institutional networks. Int J Med Inf [Internet]. 2006/11/07. 2007;76(5–6):466–70. Available from: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=17084663

5. Beech M. Confidentiality in health care: conflicting legal and ethical issues. Nurs Stand [Internet]. 2007/02/20. 2007;21(21):42–6. Available from: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=17305035

6. Rindfleisch TC. Privacy, information technology, and health care. Commun ACM. 1997;40(8):92–100.

7. Chin T. Searchers may Google your patient records. American Medical News [Internet]. 2003; Available from: http://www.ama-assn.org/amednews/2003/04/07/bisb0407.htm

8. Chin T. Computer hackers access 7,000 patient files. American Medical News [Internet]. 2003; Available from: http://www.ama-assn.org/amednews/2003/03/24/bisc0324.htm

9. Chin T. Security breach: Hacker gets medical records. American Medical News [Internet]. 2001; Available from: http://www.ama-assn.org/amednews/2001/01/29/tesa0129.htm

10. Artículo 43 de la Constitución de la Nación Argentina. 1994.

11. Ley 25236. PROTECCION DE LOS DATOS PERSONALES. Bolentin Of la República Argentina. 2006;Disposicio.

12. Interactive H. Health Information Privacy (HIPAA) Notices Have Improved Public's Confidence That Their Medical information Is Being Handled Properly [Internet]. 2005. Available from: http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=894

13. Sweeney L. k-anonymity: a model for protecting privacy. Int J Uncertain Fuzziness Knowl-Based Syst. 2002;10(5):557–70.

14. Ley 26529. Derechos del Paciente, Historica Clínica y Consentimiento Informado. Bolentin Oficial de la República Argentina 2009.

15. Record. I of MC on I the P, Dick RS, Steen EB. The computer-based patient record : an essential technology for health care. Washington, D.C.: National Academy Press; 1991. xii, 190 xii, 190 p.