Aten Primaria. 2014;46(4):214–222

Atención Primaria
www.elsevier.es/ap

ARTÍCULO ESPECIAL

Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria

Ana Sánchez-Henarejos[a,*], José Luis Fernández-Alemán[a], Ambrosio Toval[a], Isabel Hernández-Hernández[b], Ana Belén Sánchez-García[b] y Juan Manuel Carrillo de Gea[a]

[a] *Departamento de Informática y Sistemas, Universidad de Murcia, Murcia, España*
[b] *Enfermería, Servicio de Urgencias, Hospital General Universitario Reina Sofía, Murcia, España*

Recibido el 1 de junio de 2013; aceptado el 19 de octubre de 2013
Disponible en Internet el 28 de febrero de 2014

PALABRAS CLAVE
Privacidad;
Confidencialidad;
Datos personales de salud;
Buenas prácticas de seguridad;
Formación en seguridad de la información

Resumen Con la introducción de la historia clínica digital surge la necesidad de reforzar la seguridad de los datos personales de salud para garantizar su privacidad. A pesar de la gran cantidad de medidas de seguridad técnicas y de recomendaciones existentes para el ámbito sanitario, hay un aumento en las violaciones de la privacidad de los datos personales de los pacientes en centros sanitarios, en muchos casos como consecuencia de errores o descuidos de los profesionales sanitarios. En este trabajo se presenta una guía de buenas prácticas de seguridad informática en la manipulación de los datos personales de salud por parte del personal sanitario, elaborada a partir de recomendaciones, normativa y estándares nacionales e internacionales. El material presentado en este trabajo puede emplearse tanto en la formación como en auditorías de seguridad informática a trabajadores de los centros de atención primaria.

KEYWORDS
Privacy;
Confidentiality;
Personal health data;
Good security practices;
Information security training

A guide to good practice for information security in the handling of personal health data by health personnel in ambulatory care facilities

Abstract The appearance of electronic health records has led to the need to strengthen the security of personal health data in order to ensure privacy. Despite the large number of technical security measures and recommendations that exist to protect the security of health data, there is an increase in violations of the privacy of patients' personal data in healthcare organizations, which is in many cases caused by the mistakes or oversights of healthcare professionals. In this

* Autor para correspondencia.
Correo electrónico: anasanchez@um.es (A. Sánchez-Henarejos).

0212-6567/$ - see front matter
http://dx.doi.org/10.1016/j.aprim.2013.10.008

paper, we present a guide to good practice for information security in the handling of personal health data by health personnel, drawn from recommendations, regulations and national and international standards. The material presented in this paper can be used in the security audit of health professionals, or as a part of continuing education programs in ambulatory care facilities.

Introducción

En los últimos años se ha hecho un gran esfuerzo para migrar la historia clínica a formato electrónico, la llamada «historia clínica electrónica» (HCE). En España, se ha pasado de estar implantada únicamente en 2 comunidades autónomas en 2006 (Baleares y País Vasco), a disponer de una HCE de atención primaria (AP) que puede consultarse desde cualquier centro de salud de 14 comunidades autónomas en 2011, según el último informe «Las TIC en el Sistema Nacional de Salud» publicado por el Ministerio de Sanidad y Política Social[1].

La historia clínica en formato electrónico y la introducción de la telemedicina en AP[2] conllevan la necesidad de reforzar la seguridad de los datos de salud para mantener la privacidad y la confidencialidad de la información que contienen. La seguridad de la información de salud es un conjunto de medidas (administrativas, organizativas, físicas, técnicas, legales y educativas) dirigidas a protegerla frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas, con el fin de proporcionar los 3 pilares básicos: confidencialidad, integridad y disponibilidad de la misma[3].

La *confidencialidad* se refiere al proceso que asegura que la información es accesible solo para aquellos usuarios autorizados a tener acceso a la misma[4]. Es el principio básico de la política de seguridad del entorno sanitario. El acceso a esta información personal de salud debe ser estrictamente controlado de acuerdo con las consideraciones legales y éticas para asegurar que solo sea para el personal autorizado. La confidencialidad de la información sanitaria obliga al profesional de la salud a no revelar información suministrada por el paciente, o como resultado de la exploración del mismo, a cualquier otra persona[5]. Así es como lo indicó ya Hipócrates en su juramento y se exige en el Código de Ética y Deontología Médica de 2011 en su capítulo v sobre el secreto profesional[6] (artículos del 27 al 31)[6].

El segundo pilar, la *integridad*, se refiere a la obligación de garantizar que la información sea exacta y no se pueda modificar de manera no autorizada[4]. Por razones de seguridad de los pacientes, la modificación no autorizada de la información médica es un problema grave que puede repercutir en errores médicos[7].

Por último, la *disponibilidad* consiste en garantizar que se proporcione información a los usuarios autorizados en el momento en que se requiere[4]. En el entorno sanitario, el acceso a la información en el instante preciso es esencial, ya que en caso de una urgencia médica no tener la información disponible puede conllevar resultados dramáticos[5].

A la hora de garantizar la seguridad en cualquier entorno, además de tener las medidas técnicas y legales adecuadas es de vital importancia el factor humano, ya que con frecuencia los mayores problemas de seguridad se presentan por errores o descuidos en el hacer diario del personal[8].

Las organizaciones sanitarias generalmente no emplean trabajadores con habilidades en tecnologías de la información o con formación en materia de seguridad, y suelen olvidar las amenazas internas a la hora de planificar la estrategia de seguridad[5,9]. Esta situación se agrava en entornos abiertos a Internet, donde el número y la naturaleza de las amenazas van en aumento y están en continua evolución[10].

En este trabajo se lleva a cabo la identificación y selección de buenas prácticas de seguridad informática para que sirva como guía de referencia a los trabajadores de los centros de AP con acceso a un equipo informático. La selección de los estándares y la normativa de aplicación se ha realizado mediante una revisión sistemática de la literatura. Se usó la cadena de búsqueda: ((«health staff» OR «personal sanitario») AND («patient privacy» OR «patient security» OR «privacidad del paciente» OR «seguridad del paciente») AND («health information» OR «health data» OR «información de salud» OR «datos de salud») AND («act» OR «standard» OR «ley» OR «estándar»)), adaptándola a las características de los motores de búsqueda de las bases de datos consultadas: Scirus, ACM Digital Library, IEEE Digital Library y Scholar Google, entre noviembre de 2012 y julio de 2013. No se estableció ningún límite en el período de tiempo de las publicaciones consideradas en la revisión. Tras la eliminación de duplicados, la lectura del título y en ocasiones el examen parcial de los 514 documentos encontrados, se seleccionaron 12 estándares, documentos normativos y recomendaciones que estaban relacionados con las buenas prácticas de seguridad informática de los trabajadores en el ámbito sanitario. Como complemento de esta búsqueda se llevó a cabo un análisis detallado de las referencias para encontrar documentos adicionales y se revisaron las páginas web de organismos españoles para obtener normativa, recomendaciones, estudios y estándares relacionados con la materia de ámbito nacional (CCN-CERT, AEPD e INTECO). Tras esta búsqueda manual, el número final de documentos incluidos en la revisión fue de 20.

Clasificación de las amenazas a datos personales de salud

Los datos personales de salud incluyen cualquier información relacionada con un determinado paciente, ya sean en formato electrónico, escrito u oral. Suelen contener un identificador, como el nombre, la fecha de nacimiento, el número de teléfono, la dirección de correo electrónico, etc., que los relaciona con la identidad del paciente de manera inequívoca.

Según la Ley española 41/2002 reguladora de la autonomía del paciente, la historia incorporará la información

Tabla 1 Clasificación de las amenazas que pueden producir un problema de seguridad en la organización

Nivel	Clasificación de amenazas
1	*Divulgación accidental (accidental disclosure).* El trabajador sanitario, sin querer, revela información del paciente a otros. Por ejemplo, mensaje de correo electrónico enviado a la dirección incorrecta
2	*Empleado curioso.* Un trabajador con privilegios de acceso a los datos de un paciente accede a ellos por curiosidad o para sus propios fines. Por ejemplo, un profesional sanitario que accede a la información de salud de un compañero de trabajo
3	*Violación de la privacidad de los datos por un trabajador.* Miembro del personal que tiene acceso a la información de un paciente y la transmite al exterior con ánimo de lucro o por algún tipo de animadversión hacia un paciente
4	*Violación de la privacidad de los datos por un externo con intrusión física.* Un externo que entra en la instalación física y de manera forzada accede al sistema
5	*Intrusión no autorizada en la red del sistema.* Un externo, ex empleado, paciente o hacker que se introduce en la red del sistema de la organización desde el exterior y accede a la información del paciente o hace que el sistema deje de funcionar (ataque a la disponibilidad)

que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Las amenazas a la privacidad y a la seguridad de los datos personales del paciente en un centro de AP son aquellas que surgen del acceso inadecuado a estos datos, ya sea por personal interno abusando de sus privilegios o por errores no intencionados, o por agentes externos que explotan la vulnerabilidad de los sistemas de información con ataques intencionados. La tabla 1 muestra una clasificación de las amenazas de seguridad de 5 niveles, según aumenta la sofisticación de la amenaza[11,12].

Consecuencias derivadas de amenazas a la seguridad

Las amenazas son acontecimientos que pueden desencadenar un incidente en el centro de AP, produciendo impactos materiales o inmateriales en los recursos del sistema de información o relacionados con este, necesarios para que el centro funcione correctamente. Las consecuencias de estos impactos, producidos o no por una negligencia de sus trabajadores, pueden ser muy variadas y han de ser asumidas por el centro de AP[13]:

- *Daños de imagen.* Generan impacto negativo en la imagen del centro y además generan pérdida de confianza de los pacientes en el mismo.
- *Consecuencias legales.* Se enmarcan en el ámbito legal, y podrían conllevar sanciones económicas o administrativas. El centro de AP debe asumir las sanciones que le puedan ser impuestas desde la Agencia Española de Protección de Datos (AEPD) por incumplimiento de la normativa. Se debe tener en cuenta que la Ley Orgánica de Protección de Datos (LOPD)[14] establece como falta muy grave recabar y tratar datos *especialmente protegidos* sin consentimiento del afectado y vulnerar el deber de secreto sobre estos datos. La multa para este tipo de faltas oscila entre 300.506 y 601.012 euros. Cuando no existe intencionalidad, o hay factores atenuantes, como la rápida subsanación de la falta, puede ser considerada como grave, en cuyo caso oscilaría entre los 60.101 y los 300.506 euros.
- *Otras consecuencias.* Son aquellas que tienen impacto negativo en ámbitos muy diversos, como por ejemplo el ámbito político, institucional o gubernamental, entre otros. En general se trata de consecuencias que no están englobadas en los otros 2 tipos.

Tendencias actuales de las amenazas a los datos personales de salud

Existen gran cantidad de incidentes derivados de deficiencias en la seguridad de las instalaciones sanitarias, o a causa de errores o descuidos del personal en la manipulación de los datos de pacientes[15]. He aquí algunos ataques recientes, clasificados según los niveles de la taxonomía expuesta en la tabla 1.

1. *Acceso a los datos de la hija menor de una doctora que trabajaba en un centro hospitalario, por parte de trabajadores del mismo sin consentimiento de la madre* (2007)[16]. Tanto personal médico como administrativo accedieron a los datos médicos de la menor para consultar, modificar e imprimir información, sin previa autorización de su madre, trabajadora del centro (nivel 2).
2. *Cuatro mil historias clínicas de abortos se filtran en la red a través de eMule* (2008)[17]. Un empleado de una clínica, que intentaba descargarse archivos desde el ordenador del trabajo a través de eMule, pudo provocar que 11.300 historias clínicas, de ellas 4.000 de casos de aborto, terminasen expuestas a cualquier internauta (nivel 1).
3. *Un virus se introduce en los ordenadores de Sanidad* (2009)[18]. Un virus se introdujo en los ordenadores de los hospitales y centros de salud madrileños. La incidencia impidió el acceso a las historias clínicas y las analíticas de los pacientes (nivel 5).
4. *Una unidad flash fue robada del Departamento de Personal de un Hospital Provincial* (2010)[19]. La unidad contenía datos personales que fueron robados tras forzar la puerta de un despacho (nivel 4).
5. *Filtradas a través de Google 2 radiografías de pulmón de un paciente* (2011)[20]. Un grupo hospitalario español tuvo que indemnizar a un paciente que, haciendo una búsqueda por Google, encontró 2 radiografías de pulmón que se le habían practicado (nivel 3).

Además de estos casos mediáticos, existen numerosas denuncias a la AEPD por violaciones de datos derivadas de malas prácticas del personal de la organización. En 2011, la

AEPD resolvió 18 procedimientos sancionadores en sanidad por un importe de 143.204 euros[21].

En enero de 2013, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), publicó el informe *Threat Landscape. Responding to the Evolving Threat Environment*[15], que indica las tendencias en los ataques a sistemas y organizaciones del año 2012. El documento *Threat Landscape* de ENISA recoge 120 informes procedentes de la industria de la seguridad, redes de excelencia, organismos de normalización y otros, entre 2011 y 2012, y proporciona una visión de conjunto de las amenazas observadas, las que actualmente son más importantes y las tendencias emergentes en este ámbito. También identifica las 10 principales amenazas en áreas de tecnologías emergentes. Las conclusiones fueron:

1. El año 2011 se caracterizó por ser el año de las violaciones de privacidad de los datos. Aumentó el interés de los cibercriminales por atacar sistemas de información sanitarios.
2. En los últimos años el número de violaciones en la privacidad de los datos en las organizaciones sanitarias aumentó con la adopción de sistemas de historia clínica digital.
3. La mayor parte de violaciones de la privacidad de los datos se produjo a consecuencia de *negligencias de trabajadores* y por ataques externos.
4. Nueve de cada 10 violaciones se pudieron haber prevenido si las organizaciones hubiesen seguido buenas prácticas en la seguridad de los datos.
5. Entre enero y junio de 2012 el número de episodios que comprometieron la confidencialidad del sistema de información en organizaciones sanitarias casi se duplicó.
6. El 96% de todas las organizaciones sanitarias encuestadas en el informe experimentaron al menos una violación de datos en los últimos años.

Por tanto, es crucial vigilar y actualizar los hábitos de seguridad del personal con acceso a los sistemas informáticos de la organización sanitaria.

Revisión de las recomendaciones de seguridad informática del entorno sanitario

En la tabla 2 se identifican y numeran algunas de las recomendaciones de organismos oficiales nacionales e internacionales, normas y estándares de seguridad aplicables a los entornos de AP y que han sido seleccionados para la elaboración de la guía de buenas prácticas de seguridad informática que aborda este trabajo.

Además de estas recomendaciones, en el año 2014 está prevista la entrada en vigor de la nueva directiva europea de protección de datos de carácter personal[22], que podría suponer cambios en la guía presentada en este trabajo.

Guía de buenas prácticas de seguridad informática para el personal de atención primaria

En la tabla 3 se presenta la guía de buenas prácticas informáticas obtenida de las recomendaciones, normas y estándares

Tabla 2 Estándares, normas y recomendaciones de seguridad para el ámbito de los centros de atención primaria

Estándares

1. Estándar ISO 27002 Security techniques — Code of practice for information security management
2. Estándar ISO 27799 Information security management in health using ISO/IEC 27002

Recomendaciones de organismos oficiales

Health Information Technology. Organización para la formación en seguridad y privacidad de los datos personales de salud. Depende del Department of Health & Human Services de EE. UU.

3. Guide to Privacy and Security of Health Information. The Office of the National Coordinator for Health Information Technology. Department of Health and Human Services, EE. UU.

Instituto Nacional de Tecnologías de la Comunicación (INTECO)

4. Recomendaciones para la creación de una contraseña segura, 20 de noviembre de 2012

Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT)

5. Guía de Seguridad (CCN-STIC-803) Esquema Nacional de Seguridad. Valoración de los Sistemas 2011
6. Guía de seguridad (CCN-STIC-821) Esquema Nacional de Seguridad. Normas de seguridad. 2012
7. CCN-STIC-821.Apéndice I. Normativa General de Utilización de los Recursos y Sistemas de Información. NG00
8. CCN-STIC-821. Apéndice II. Normas de acceso a Internet. NP10
9. CCN-STIC-821. Apéndice III. Normas de uso del correo electrónico (e-mail). NP20
10. CCN-STIC-821. Apéndice IV. Normas de Seguridad en el ENS. Normas para trabajar fuera de las instalaciones. NP30
11. CCN-STIC-821. Apéndice V. Normas de creación y uso de contraseñas. NP40
12. CCN-STIC-821. Apéndice VI. Acuerdo de confidencialidad para terceros. NP50
13. CCN-STIC-821. Apéndice VII. Modelo de contenido de buenas prácticas para terceros. NP60

NIST (National Institute of Standards and Technology)

14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule 2009
15. Guide to Enterprise Password Management Recommendations of the National Institute of Standards and Technology

Normas

HIPAA (Health Insurance Portability and Accountability Act). Ley Federal de EE.UU.

16. HIPAA Handbook for Behavioral Health Staff: Understanding the Privacy and Security Regulations. En: Congress US, editor. 2009
17. Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

Tabla 2 (*continuación*)

18. Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica
19. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
20. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

revisados, dividida en bloques según la temática que abarca. La guía está orientada tanto al personal sanitario como al no sanitario, siempre y cuando empleen un ordenador con acceso a datos personales del paciente. La tercera columna indica la amenaza que previene cada recomendación, atendiendo a la clasificación presentada en la tabla 1. En la última columna se indica la fuente de la que se ha extraído la recomendación en base a la numeración dada en la tabla 2. En las siguientes líneas se justifica cada bloque y se ofrecen recomendaciones prácticas para los profesionales.

Recomendaciones de formación

La formación es la mejor forma de concienciar a los trabajadores sobre los riesgos de seguridad, las posibles consecuencias de incidentes y la responsabilidad de estos en los mismos, así como las principales medidas de prevención. Es por tanto fundamental que el centro de AP cuente con un plan de formación periódico, actualizado y con material estandarizado.

Recomendaciones de contraseña

La composición y la privacidad de la contraseña son factores cruciales para mantener la eficacia de este mecanismo de protección frente accesos no autorizados al sistema de información sanitario. El profesional debe elegir una contraseña que cumpla las recomendaciones presentadas en la tabla 3, pero que sea fácil de recordar aplicando alguna regla sencilla que solo él conozca. De este modo se evita tener que anotar la contraseña para recordarla. Se pueden utilizar comprobadores de contraseña fiables para conocer el nivel de seguridad de la contraseña. La contraseña no debe aparecer ni ser compartida por ningún medio para evitar que alguien suplante su identidad. No se debe proteger varias cuentas con la misma contraseña, pues si la contraseña es descubierta, podrán suplantar la identidad del profesional en todas las cuentas. Finalmente, la primera vez que se accede a un sitio web nunca se debe responder sí a la pregunta del navegador: «¿Desea guardar su contraseña?». Si otro usuario del equipo accede de nuevo al mismo sitio web, podrá suplantar su identidad.

Recomendaciones de uso de certificado digital

Un certificado digital es un conjunto de datos que permiten la identificación del titular del certificado ante terceros, intercambiar información con otras personas y entidades de manera segura, y firmar electrónicamente los datos que se envían, manteniendo su integridad y conociendo su procedencia. Su uso se está generalizando desde la entrada en vigor del DNI electrónico, y requiere una contraseña que debe ser mantenida bajo las reglas del apartado anterior.

Recomendaciones de uso del correo electrónico

Como regla general, nunca se debe utilizar el correo electrónico para intercambiar datos de salud, y si fuera imprescindible, siempre debe hacerse entre cuentas corporativas de la organización de salud, firmando y cifrando los datos trasmitidos utilizando un certificado electrónico, e incluyendo una cláusula de confidencialidad advirtiendo de la naturaleza sensible de la información. Se debe evitar abrir archivos adjuntos o pinchar en enlaces recibidos a través del correo electrónico, aunque procedan de cuentas de personas conocidas. Bajo estos archivos puede haber software malicioso (los troyanos) que acceda, controle y dañe la información del ordenador bajo una apariencia inocua, sin que sea advertido por el profesional sanitario.

Recomendaciones de uso y acceso a Internet e Intranet

La visualización de un vídeo, el ingreso en un enlace encontrado en una red social, en una ventana emergente de un anuncio o tras una simple búsqueda on-line, puede poner en peligro la seguridad y la privacidad de los datos sanitarios. Es fundamental que el trabajador esté informado de cuáles son las buenas prácticas de navegación por Internet y siga algunos consejos básicos: disponer de herramientas de seguridad (antivirus, firewall, antispam) actualizadas; realizar análisis con el antivirus periódicamente; no descargar ni ejecutar ningún archivo de sitios desconocidos, pues puede incluir software malicioso; nunca entregar datos personales o circunstancias familiares a desconocidos o en páginas no seguras (que no comiencen por https://); no aceptar contactos desconocidos en redes sociales y mensajería instantánea; nunca pulsar el botón aceptar de una ventana sin leer y entender el mensaje, y finalmente buscar un técnico informático para actualizar y configurar el navegador y el sistema operativo de forma segura.

Recomendaciones de uso de dispositivos extraíbles

Conectar un dispositivo extraíble a un ordenador del centro de AP supone un riesgo alto de entrada de virus a la Intranet del centro. Para evitar infecciones, no se deben conectar dispositivos extraíbles que hayan sido utilizados en otros equipos informáticos. Hay que cifrar con un certificado digital la información que salga del centro, y cuando ya sea desechable, hacer un borrado irreversible con alguna utilidad de borrado seguro. Estas aplicaciones incluyen funciones para limpiar el área de memoria ocupada por los ficheros, con el fin de no dejar rastro de la información generada y almacenada en su ordenador durante su uso (contraseñas, datos personales, etc.).

Tabla 3 Guía de buenas prácticas para la seguridad informática en centros de AP. Para cada recomendación se especifica el nivel de amenaza prevenido y la fuente de la que procede según la numeración de la Tabla 2

Bloque	Recomendación	Amenaza prevenida	Estándares, normas y recomendaciones (tabla 2)
Formación	Se debe conocer y aplicar la política de seguridad de la organización sanitaria que debe estar definida según lo dispuesto en el artículo 11 del Esquema Nacional de Seguridad	Nivel 1, 4, 5	1,2,16,20
Fortaleza contraseñas	La contraseña se debe modificar cada 90 días	Nivel 1, 2, 4, 5	11,16
	La contraseña debe estar compuesta por 8 dígitos como mínimo	Nivel 1, 2, 4, 5	4,11,15,16
	Componerla de letras mayúsculas y minúsculas, algún número y algún carácter especial	Nivel 1, 2, 4, 5	1,4,11,15,16
	La contraseña no debe constar de fechas, nombres o información personal	Nivel 1, 2, 4, 5	1,4,11,15,16
	La contraseña no debe apuntarse en ningún sitio ni enviarla por correo electrónico	Nivel 1, 2, 4, 5	1,4,11,15,16
	La contraseña debe de ser diferente de la que protege cuentas de carácter personal	Nivel 1, 2, 4, 5	1,4,11,15,16
	No compartir la contraseña con nadie ni solicitar la de otro compañero	Nivel 1, 2, 3, 4, 5	1,4,11,15,16
	No guardar la contraseña en el navegador de Internet	Nivel 1, 2, 3, 4, 5	1,4,11,15,16
Uso de certificados digitales	Los certificados digitales deben protegerse con contraseña y aplicarle a esta las mismas reglas del bloque anterior	Nivel 1, 2, 3, 4, 5	20
Uso del correo electrónico	No consultar cuentas de correo personal desde el centro sanitario por ser una posible entrada de virus y fuga de información	Nivel 1, 3, 5	1
	No enviar desde cuentas de correo personal información personal de salud, ni proporcionar la dirección para recibir este tipo de datos	Nivel 1, 3, 5	1
	No utilizar su cuenta de correo electrónico corporativa para fines personales, y extremar las medidas de seguridad si va a acceder a ella desde un domicilio particular	Nivel 1, 3, 5	1,9
	No responder a correos electrónicos que le soliciten la remisión de datos de salud	Nivel 1, 2, 3, 5	1,9,16
	Extremar la precaución, al abrir adjuntos de un correo electrónico para no introducir virus en el centro.	Nivel 1,5	1,9,16
	Encriptar o codificar los correos electrónicos que contengan datos personales de salud	Nivel 1, 2, 5	1,2,9,16
	Incluir en el pie de los faxes y correos electrónicos enviados una cláusula informando de la naturaleza y privacidad de los datos	Nivel 1	1,2,9,16
Acceso a Internet	Evitar navegar por: redes sociales, páginas de descargas, páginas de almacenamiento de archivos, mensajería instantánea y juegos online por ser una entrada potencial de amenazas	Nivel 1, 3, 5	1,16
	Precaución en la descarga de archivos de Internet	Nivel 1, 2, 5	1,16
Uso de dispositivos y medios extraíbles	Consultar con el responsable de la información la conveniencia o no de sacar información personal de salud del centro en un medio extraíble	Nivel 1, 3, 4, 5	1,6,16,19
	Encriptar o codificar la información personal de salud que salga del centro en medios extraíbles o dispositivos portátiles	Nivel 1, 3, 4, 5	2,10,16,19
	Precaución en el uso de medios extraíbles (USB, CD) para evitar la entrada de virus	Nivel 1, 3, 5	10,16,19

Tabla 3 (*continuación*)

Bloque	Recomendación	Amenaza prevenida	Estándares, normas y recomendaciones (tabla 2)
	Borrado seguro de medios extraíbles con información personal de salud al desecharse para evitar que pueda recuperarse	Nivel 1, 3, 4, 5	1,2,10,16,19
Uso de equipos	Cerrar la sesión, bloquearla o apagar la pantalla del ordenador cuando vaya a ausentarse del mismo durante 5 min o más	Nivel 1, 2, 3, 4, 5	1,2,7,16
	Evitar que los datos desplegados en pantallas sean vistos por personas no autorizadas	Nivel 1, 2, 3, 4, 5	1,2,16
	No colocar información sensible en unidades del ordenador compartidas con trabajadores que no tengan autorización a acceder a dichos datos	Nivel 1, 2, 3, 4, 5	1
	Acceder únicamente a la información indispensable para desempeñar el trabajo. Si se accede a información que no deba ser vista, se debe informar al departamento de informática del centro	Nivel 1, 2, 3, 4, 5	1,16
	Borrar la memoria de las fotocopiadoras de alta capacidad del centro tras fotocopiar información que contenga datos personales de salud	Nivel 1, 2, 3, 4, 5	1
	Retirar los documentos con datos sensibles de la bandeja de impresión de las impresoras y faxes para que no puedan ser consultados por personal no autorizado	Nivel 1, 2, 3, 4, 5	1,7,16
Instalación de software	No instalar software no relacionado con las funciones del puesto de trabajo por ser una posible entrada de amenazas	Nivel 1, 3, 5	7,16
	Cuidar que el software a instalar esté libre de virus	Nivel 1, 3, 5	1,16
Incidencias de seguridad	Conocer el protocolo de actuación frente a la detección de amenazas informáticas	Nivel 1, 2, 3, 4, 5	1,16
	Informar de cualquier anomalía en el funcionamiento del ordenador a quien corresponda según el procedimiento que debe ser definido por la organización para la notificación de incidencias	Nivel 1, 2, 3, 4, 5	1,16

Recomendaciones de uso de equipos informáticos

La medida más segura para proteger la pantalla de visualización de datos y otros periféricos cuando se ausente, es bloquear el ordenador con una contraseña. Asimismo hay que borrar los documentos de la memoria de impresoras y fotocopiadoras utilizando las opciones de ajuste y configuración particulares de cada dispositivo. Especial precaución se debe tener al depositar ficheros en directorios o dispositivos compartidos con otros usuarios, de manera que solo accedan a la información usuarios autorizados. En el caso de advertir alguna circunstancia en la que usuarios no autorizados puedan acceder a datos personales de salud, se debe comunicar inmediatamente al Departamento de Informática del centro de AP.

Recomendaciones de instalación de software

Desconfiar del software disponible en Internet, pues suele contener software malicioso e incluso software espía que pone en riesgo los datos personales de salud. Preferentemente, descargar software procedente de webs oficiales, utilizar un antivirus y siempre consultar antes con un técnico informático. Para disminuir riesgos, evitar la instalación de software no relacionado con el puesto de trabajo en su centro de AP.

Recomendaciones de incidencias de seguridad

Es crucial concienciar a los trabajadores de la necesidad de comunicar los problemas de seguridad en el equipamiento informático del centro de AP, de manera que la organización establezca las medidas correctivas pertinentes para minimizar el impacto de las incidencias de seguridad y subsanar los daños derivados del mismo.

Formación en buenas prácticas de seguridad informática para el profesional de atención primaria

La formación en materia de seguridad y privacidad de los trabajadores de los centros de AP es de vital importancia[23,24],

tanto para la confidencialidad y privacidad de los datos del paciente como para el centro de AP, que en caso de negligencia de sus trabajadores, deberá asumir las consecuencias del impacto de seguridad derivado de la misma.

Como se suele decir, la prevención es la mejor medicina, y poner en práctica las recomendaciones presentadas en este trabajo puede reducir en gran medida los incidentes de seguridad y, por tanto, los riesgos de violación de datos personales del centro. Se ha demostrado que la inversión en formación del personal sanitario en materia de seguridad reduce el riesgo de sufrir incidentes de seguridad[23], que incluso pueden afectar al cuidado asistencial[25]. Por esta razón, es recomendable adoptar material educativo estandarizado[26] procedente de organizaciones acreditadas, como *Health Information Technology* (HealthIT). Esta organización ofrece un sitio donde el profesional de la salud puede recibir toda la información práctica en materia de seguridad para el desempeño de su actividad. HealthIT pone a disposición pública aplicaciones on-line como Cybersecure[27], en las que el profesional de la salud puede ir evaluando sus conocimientos en materia de seguridad y privacidad conforme a la legislación estadounidense, mediante la resolución de diferentes casos prácticos organizados por semanas. Pese a estar basado en la legislación estadounidense, la mayoría de las recomendaciones son igualmente aplicables en España.

Conclusiones

Debido a la gran cantidad de procedimientos, normativa y estándares disponibles para la protección de los datos, y a las dificultades técnicas inherentes a la informática, resulta difícil para los trabajadores sanitarios encontrar una referencia o documento que reúna las buenas prácticas de seguridad informática en el tratamiento de datos de salud. Además, las amenazas de seguridad a las que se enfrentan las organizaciones sanitarias no son nada desdeñables, y su control depende en gran medida de la política de seguridad de la organización. La formación de cada uno de los trabajadores en materia de seguridad y privacidad de la información es crucial para evitar errores que comprometan el sistema informático de la organización. Por tanto, es de vital importancia vigilar y actualizar los hábitos de seguridad del personal con acceso a los sistemas informáticos de la organización sanitaria.

La guía presentada en este artículo pretende ser una orientación sobre buenas conductas y hábitos del personal sanitario en el tratamiento de los datos, y ayudar en la formación de estos profesionales. Esta guía puede ser utilizada para evaluar y auditar[28] el comportamiento en materia de seguridad del trabajador por parte de los responsables de seguridad informática del centro de AP.

Financiación

Este trabajo forma parte del proyecto PEGASO-PANGEA (TIN2009-13718-C02-02), financiado por el Ministerio de Ciencia e Innovación, y del proyecto GEODAS-REQ (TIN2012-37493-C03-02), financiado por el Ministerio de Economía y Competitividad y con fondos europeos FEDER.

Conflicto de intereses

Los autores declaran no tener ningún conflicto de intereses.

Bibliografía

1. Ministerio de Sanidad y Política Social. Las TIC en el Sistema Nacional de Salud (SNS): El programa Sanidad en Línea. Madrid 2010 [consultado Ago 2013]. Disponible en: http://www.ontsi.red.es/ontsi/es/estudios-informes/las-tic-en-el-sistema-nacional-de-salud-ed-2010
2. Prados Castillejo JA. Telemedicina, una herramienta también para el médico de familia. Aten Primaria. 2013;45:129–32.
3. CCN-CERT. Esquema Nacional de Seguridad. Guía de Seguridad (CCN-STIC-800). Esquema Nacional de Seguridad. Glosario de Términos y Abreviaturas. Centro Criptológico Nacional. 2011 [consultado Ago 2013]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/800-Glosario_de_terminos_y_abreviaturas/800-Glosario_de_terminos_ENS-mar11.pdf
4. ISO/EN 13606. Health informatics — Electronic health record communication [consultado Ago 2013]. Disponible en: http://www.iso.org/iso/home.htm
5. Patricia A.W. Medical insecurity: When one size does not fit all. The 5th Australian Information Security Management Conference Edith Cowan University. Australia. 2007 [consultado Ago 2013] Disponible en: http://roecueduau/cgi/viewcontentcgi?article=1043&context=ism
6. Consejo General de Colegios Oficiales de Médicos. Código Deontología Médica. Guía Ética Médica. Madrid 2011 [consultado Ago 2013]. Disponible en: https://www.cgcom.es/sites/default/files/codigo_deontologia_medica.pdf
7. Fernández-Alemán JL, Señor IC, Lozoya PAO, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform. 2013;46:541–62.
8. Colwill C. Human factors in information security: The insider threat — Who can you trust these days? Information Security Technical Report. 2009;14:186–96.
9. Williams PAH. In a 'trusting' environment, everyone is responsible for information security. Information Security Technical Report. 2008;13:207–15.
10. Alban RF, Feldmar D, Gabbay J, Lefor AT. Internet security and privacy protection for the health care professional. Curr Surg. 2005;62:106–10.
11. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Commission on Physical Sciences, Mathematics, and Applications, National Research Council. For the Record: Protecting Electronic Health Information. National Academy Press. Washington 1997 [consultado Ago 2013]. Disponible en: http://www.nap.edu/openbook.php?record_id=5595
12. Appari A, Johnson ME. Information security and privacy in healthcare: Current state of research. International Journal of Internet and Enterprise Management. 2010;6:279–314.
13. INTECO. Guía para la gestion de fuga de información. Ministerio de Industria, Energía y Turismo. Mayo 2012 [consultado Ago 2013]. Disponible en: http://www.inteco.es/guias/guia_fuga_informacion
14. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Madrid 1999 [consultado Ago 2013]. Disponible en: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf
15. European Network and Information Security Agency. ENISA Threat Landscape Responding to the Evolving Threat Environment [consultado Ago 3013]. Disponible en: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport

16. Resolución de archivo de actuaciones del Expediente E/00562/2007 de la Agencia Española de Protección de Datos. Madrid 2008 [consultado Ago 2013]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2008/common/pdfs/E-00562-2007_Resolucion-de-fecha-07-04-2008_Art-ii-culo-9-LOPD.pdf
17. Ceberio Belaza M. 4.000 historias clínicas de abortos se filtran en la Red a través de eMule. El País digital. Madrid: Ediciones El País S.L. 2008 [consultado Ago 2013]. Disponible en: http://elpais.com/diario/2008/04/25/sociedad/1209074403_850215.html
18. Sevillano EG. Un virus se cuela en los ordenadores de Sanidad. El País digital. Madrid: Ediciones El País S.L. 2009 [consultado Ago 2013]. Disponible en: http://elpais.com/diario/2009/05/12/madrid/1242127454_850215.html
19. Resolución R/01436/2010 de la Agencia Española de Protección de Datos. Madrid 2010 [consultado Ago 2013]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/admon_publicas/ap_2010/common/pdfs/AAPP-00018-2010_Resolucion-de-fecha-02-07-2010_Art-ii-culo-9-20-LOPD.pdf
20. Resolución R/02338/2011 de la Agencia Española de Protección de Datos. Madrid 2011 [consultado Ago 2013]. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2011/common/pdfs/PS-00417-2011_Resolucion-de-fecha-09-12-2011_Art-ii-culo-9.1-LOPD.pdf
21. AEPD. Memoria de la Agencia Española de Protección de Datos. Madrid 2012 [consultado Ago 2013]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf
22. Saracci R, Olsen J, Seniori-Costantini A, West R. Epidemiology and the planned new Data Protection Directive of the European Union: A symposium report. Public Health. 2012;126:253–5.
23. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study. J Med Syst. 2010;34:629–42.
24. 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. Comput Methods Programs Biomed. 2010;99:230–51.
25. Fernando JI, Dawson LL. The health information system security threat lifecycle: An informatics theory. Int J Med Inform. 2009;78:815–26.
26. Wiljer D, Urowitz S, Apatu E, DeLenardo C, Eysenbach G, Harth T, et al. Patient accessible electronic health records: Exploring recommendations for successful implementation strategies. J Med Internet Res. 2008;10:e34.
27. The Office of the National Coordinator for Health Information Technology's Office of the Chief Privacy Officer. Cybersecure: Your medical practice U S Department of Health & Human Services 2012 [consultado Ago 2013]. Disponible en: http://www.healthit.gov/sites/default/files/cybersecure/cybersecure.html
28. Martínez MA, Lasheras J, Fernández-Medina E, Toval A, Piattini M. A personal data audit method through requirements engineering. Computer Standards & Interfaces. 2010;32:166–78.