INVESTIGACIÓN

La seguridad de la información, clave en la protección de datos sanitarios

Karina Ingrid Medinaceli Díaz* y Eugenio Gil**

RESUMEN

La informatización de la historia clínica ha hecho necesario adoptar nuevas medidas de seguridad para el control de accesos y del uso de la información que se encuentra en los ordenadores, tratando de preservar así la intimidad de los pacientes. La historia clínica electrónica no es menos segura ni garantiza menos la confidencialidad que la historia en papel, existen procedimientos para garantizar esa seguridad y confidencialidad, que por otro lado exigen tanto la normativa sanitaria (Ley 41/2002) como la de protección de datos (Ley 15/1999). Esos procedimientos son los que permiten garantizar la identidad de la persona que accede, la autorización con que cuenta, la disponibilidad de la información, la integridad de ésta y el no repudio a las anotaciones o consultas llevadas a cabo en la historia.

PALABRAS CLAVES: <Ley Orgánica de Protección de Datos de Carácter Personal><Confidencialidad en datos de salud><Seguridad de la información><Tecnologías de la información y comunicación>

The security of the information, key in the protection of sanitary data

SUMMARY

The automatization of clinical history has done necessary to adopt new safety measures for the control of accesses and the use of the information that is in the computers, being treated to preserve therefore the privacy of the patients. Electronic clinical history is less safe neither guarantees the less the confidentiality that history in paper, exists procedures to guarantee that security and confidentiality, that on the other hand demand so much the sanitary norm (Law 41/2002) like the one of protection of data (Law 15/1999). Those procedures are those that allow to guarantee the identity of the person who accedes, the authorization whereupon it counts, the availability of the information, the integrity of this and not repudio to the annotations or carried out consultations in history.

Key words: <Statutory law of Protection of Data of Carácter Personal><Confidentiality data of health><Security of the information><Technologies of the information and communications>

* Karina Medinaceli. Abogada, Máster en Informática y Derecho por la Universidad Complutense de Madrid (España), Candidata a Doctor del Doctorado en Informática, Programa Sociedad de la Información y del Conocimiento por la Universidad Pontificia de Salamanca (España), Docente Titular de Derecho Informático en la Facultad de Derecho y Ciencias Políticas de la Universidad Mayor de San Andrés. karina.medinaceli@gmail.com

** Eugenio Gil. Abogado, Doctor en Ingeniería Informática, Programa Sociedad de la Información y del Conocimiento por la Universidad Pontificia de Salamanca (España), Docente de Derecho Informático en la Facultad de Informática de la Universidad Pontificia de Salamanca. eugenio.gil@upsam.es

Introduccion

La irrupción de las nuevas tecnologías en la sociedad a través de su aplicación en ámbitos como el medio ambiente, el científico, la ingeniería o las comunicaciones es un hecho manifiesto. El sector sanitario no ha podido sustraerse a esta realidad y ha visto renovadas muchas de sus estructuras tradicionales con las nuevas opciones traídas por la aplicación de las tecnologías de la información y comunicaciones (TIC) en sectores como la gestión y la administración hospitalaria, a través de la creación de bases de datos para almacenar la información hasta ahora recopilada en archivos de difícil acceso, o posibilitando proyectos como la historia clínica electrónica.

Revisamos el régimen jurídico internacional, comunitario y particularmente la normativa de España para el tratamiento de los datos personales en el ámbito sanitario, calificados por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), como especialmente protegidos, haciendo que se tenga una necesaria reserva y custodia de los datos personales de los pacientes que al incorporarse a soportes informáticos, exigen un especial deber de diligencia para evitar que puedan ser conocidos por personas ajenas al proceso asistencial o no habilitadas por la ley.

La utilización de las TIC en el ámbito de los datos sanitarios puede generar, si se separa de los criterios que lícitamente han de guiarla, atentados contra derechos fundamentales de la persona, su derecho a la intimidad y el control que ésta puede ejercer sobre sus datos personales.

El Real Decreto 1790/2007 Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal establece las medidas técnicas y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamientos, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos personales.

La seguridad de la información clínica esta garantizada con las actuales tecnologías de la información y comunicaciones contando para ello con medidas de seguridad como software seguro, TIC en seguridad (back up, accesos lógico y físico, cifrado, redundancia, cortafuegos y proxies, reserva), firma electrónica, auditorías informáticas, sistema de gestión de seguridad de la información, entre otros. Se presume que la aplicación de las TIC añade eficiencia y aumenta la calidad de las prestaciones pero son necesarias más evaluaciones que aseguren este punto o pongan de manifiesto los nuevos problemas generados por su uso.

En la presente comunicación queremos dar a conocer que hoy en día existen medidas de seguridad que brindan las TIC y que resguardan la confidencialidad en el tratamiento de los datos personales en el ámbito sanitario.

Protección de datos sanitarios

La materia de protección de datos sobre personas físicas empezó a ser tomada en serio en el momento de redactar la Constitución española, pues ya en su artículo 18.4 se prevé que algún día deberá regularse el tratamiento automatizado de datos de las personas.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) tiene por finalidad principal incorporar al dere-

cho interno español la Directiva 95/46/CE, aunque no se diga expresamente en la LOPD, porque carece de exposición de motivos e incluso de un simple preámbulo.

El ámbito de la LOPD abarca los datos de carácter personal registrados en soporte físico, no necesariamente ficheros informatizados, que los hace susceptibles de tratamiento y toda modalidad de uso posterior de los mismos por los sectores público y privado; como novedad incluye al derecho de oposición y se caracteriza por ser una normativa matizada por numerosas excepciones.

Antes de comentar y explicar los datos especialmente protegidos, es necesario aclarar qué son los datos de carácter personal. Estos, según la Recomendación No. R (83)10 del Comité de Ministros del 23 de septiembre, son todos aquellos que proporcionan información referente a una persona física identificada o identificable. Una persona física no se considerará identificable si dicha identificación exige un tiempo y unas actividades no razonables. La LOPD, en su artículo 3, los define como "cualquier información concerniente a personas físicas identificadas o identificables".

Cuando los datos de carácter personal, además de tener las características de éstos, expresan una información sobre el origen racial, las convicciones de ideología, religión o creencias, la salud o la vida sexual, han venido denominándose datos sensibles, éstos son objeto de una protección especial y son definidos en el artículo 7 de la LOPD como datos especialmente protegidos.

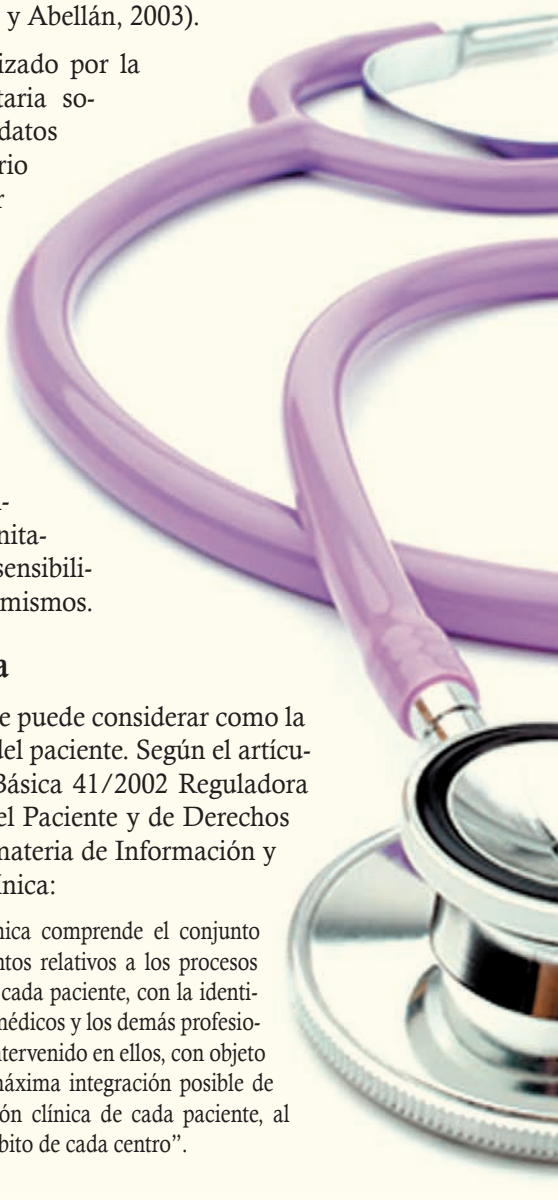
Respecto de los datos sanitarios este régimen de especial protección se concreta, básicamente, en que los mismos sólo podrán ser recabados, tratados y cedidos en los términos que establece la LOPD, también en el hecho de que los citados datos son merecedores de la adopción de medidas técnicas de seguridad de nivel alto (Sánchez-Caro y Abellán, 2004).

Los datos médicos o de salud como concepto amplio no está definido en la legislación española, comprende todos los datos que de alguna forma se refieran a la salud tanto de las personas con buena salud, enfermos o fallecidos, por lo que se debe evitar una definición pormenorizada que deje fuera información que puede incidir sobre la salud de la persona y que de no contemplarse le pueda generar situaciones de indefensión y de potencial agresión contra sus derechos particulares (De Miguel, 2004).

En consecuencia siendo lo más extensos posible para poder abarcar un concepto amplio y expansivo de qué se debe entender por datos médicos o de salud, quedarán comprendidos, todos aquellos datos que tienen que ver con el cuerpo humano, como la sexualidad, la raza, el código genético, los antecedentes familiares, los hábitos de vida, de alimentación y consumo; los datos antropométricos como peso, talla y edad; las enfermedades actuales, pasadas o futuras previsibles, bien sean de tipo físico o psíquico; las informaciones relativas al abuso de alcohol o al consumo de drogas; los datos administrativos de los centros sanitarios; y los aspectos económicos relacionados con la prestación de la asistencia sanitaria (Sánchez Carazo, 2000).

En el ámbito internacional hay una conciencia generalizada sobre la importancia y complejidad que encierran las prácticas de tratamiento de datos de salud, partiendo desde el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, sobre la protección de las personas en lo que respecta al tratamiento automatizado de sus datos de carácter personal; la Recomendación Nº R (97) 5, de 13 de febrero, relativa a la protección de datos médicos, que presta una atención especial a los datos genéticos; el Convenio relativo a los Derechos Humanos y la Biomedicina (también conocido como Convenio de Oviedo), de 4 de abril de 1997, que presta una especial atención a las cuestiones relativas al genoma humano; y la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de datos de las personas físicas en lo que respecta a su tratamiento y a la libre circulación de los mismos (Sánchez-Caro y Abellán, 2003).

Este recorrido realizado por la normativa comunitaria sobre protección de datos en el ámbito sanitario nos permite percibir una constante preocupación por la protección del derecho a la intimidad en el tratamiento de datos personales, prestándose una atención particular a los datos sanitarios por la especial sensibilidad conferida a los mismos.



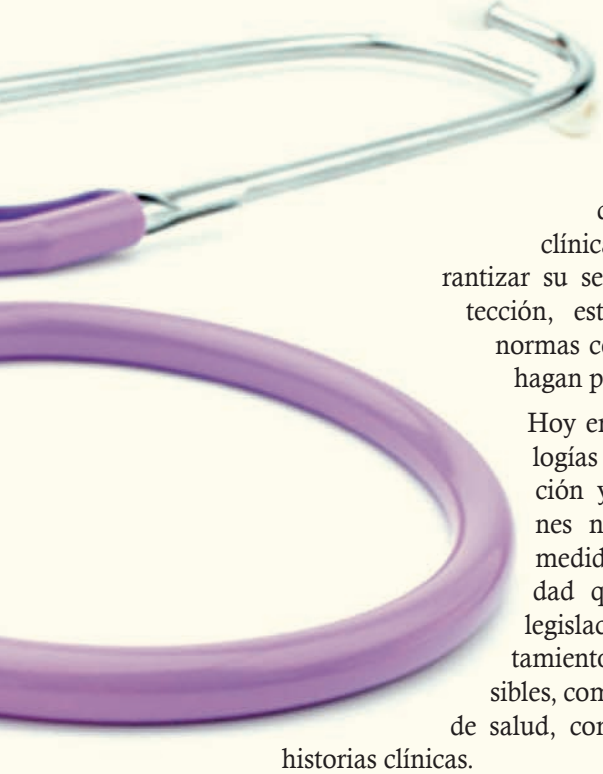
La historia clínica

La historia clínica se puede considerar como la biografía sanitaria del paciente. Según el artículo 14.1 de la Ley Básica 41/2002 Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica:

> "la historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos en el ámbito de cada centro".

Existe consenso por parte de muchos autores en considerar la historia clínica como uno de los documentos médicos más complejos que existen, debido a la diversidad de personas y organismos que en un determinado momento pueden estar interesados en tener acceso a los datos en ella contenidos, lo que compromete la intimidad del paciente. No se debe olvidar que los bienes y valores que se relacionan a la historia clínica son de una importancia extraordinaria ya que están directamente relacionados con derechos fundamentales de la persona como el derecho a la intimidad, a la salud, a la libertad y a la confidencialidad (De Miguel, 2002).

La Ley 41/2002 otorga la base legal para que se pueda tener una historia clínica única, lo más completa posible, donde estarán contenidos todos los episodios asistenciales que pueda tener el paciente a lo largo de toda su vida. La ley también establece que el centro sanitario es el responsable del adecuado archivo, conservación y disponibilidad de la historia clínica debiendo garantizar su seguridad y protección, estableciendo las normas concretas que lo hagan posible.



Hoy en día las tecnologías de la información y comunicaciones nos ofrecen las medidas de seguridad que requiere la legislación para el tratamiento de datos sensibles, como son los datos de salud, contenidos en las historias clínicas.

El responsable del fichero en el ámbito sanitario

La determinación de quién es el responsable del fichero de historias clínicas o de datos sanitarios es de gran importancia porque será éste el obligado a declarar los ficheros, será él ante quien se ejerciten los derechos de acceso, rectificación y cancelación y es también quien va a responder ante la posible infracción que se cometa en este ámbito.

La LOPD señala que el Responsable del Fichero será la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento de los datos personales.

El Real Decreto 1277/2003, de 10 de octubre, define a los centros y servicios de titularidad pública como:

> "el conjunto organizado de medios técnicos e instalaciones en el que profesionales capacitados, por su titulación oficial o habilitación profesional, realizan básicamente actividades sanitarias con el fin de mejorar la salud de las personas".

En este sentido la Ley 41/2002 aporta luces al establecer que la gestión de la historia clínica por los centros se realiza a través de la Unidad de Admisión y Documentación Clínica, encargada de integrar en un solo archivo las historias clínicas, estando bajo la dirección del centro sanitario la custodia de las mismas, por tanto, en los centros sanitarios corresponde al gerente la responsabilidad del fichero de historias clínicas. En el caso de profesionales sanitarios que desarrollan su actividad de manera individual, son ellos los responsables de la gestión y de la custodia de la documentación asistencial que generan (Sánchez-Caro y Abellán, 2003).

Seguridad de la información

Si miramos la norma PNE – 150/IEC 27002 "Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información", encontramos que nos recuerda que la información es un activo que hay que proteger, y que puede estar en diferentes tipos de soportes. La norma citada sigue manteniendo tres vertientes clásicas de la seguridad:

- *Confidencialidad:* garantizando que la información protegida sólo es accesible (o sólo puede ser revelada) a quienes están autorizados al acceso.
- *Integridad:* garantizando que la información y sus métodos de proceso son exactos y completos, y podríamos matizar que, por tanto, permitiendo el acceso con posibilidad de variación, que incluiría añadidos, modificaciones y supresiones, pero sólo a quienes estén autorizados, y que podrían ser diferentes del grupo anterior el de la confidencialidad.
- *Disponibilidad:* garantizando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Podemos entender que la disponibilidad sería dentro de un marco de tiempo, variable según el sector y tipo de aplicación, y que una situación de no disponibilidad temporal es un riesgo, generalmente mucho menor que la no disponibilidad definitiva por pérdida irreversible de la información correspondiente.

La implantación de controles disminuye el riesgo, esos controles dependerán del tipo de activo a proteger y de las amenazas a que esté sometido, y pueden ser generales o más específicos, y humanos o técnicos, así como tangibles y físicos, o bien de tipo lógico (Aceituno, 2004).

El problema de la protección de datos personales puede ser más difícil que la protección de otros activos o bienes, porque las comunicaciones y especialmente a través de internet, cuando son los datos accesibles por este medio y no existe protección adecuada, pueden existir accesos indebidos desde cualquier parte del mundo y las 24 horas del día. Por otra parte, al contrario de lo que ocurre con otros activos, la copia tiene el mismo valor que el original, lo que es excelente pensando en asegurar la disponibilidad y a veces la integridad mediante las copias de respaldo. Pero a la vez es un riesgo añadido, porque quien logre acceder a los datos y copiarlos, y probablemente sin dejar pistas o borrándolas, tendrá el mismo valor que el original, aunque con el tiempo la copia pueda perder actualidad (Del Peso, 2003).

La seguridad es muy amplia, pero en la presente comunicación nos ceñimos a la de los datos, y además de carácter personal, con frecuencia nos referimos a datos e información en la vida cotidiana casi de forma indistinta, pero para ser más precisos tenemos que diferenciarlos.

La LOPD, en su artículo 3, define datos de carácter personal como: "Cualquier información concerniente a personas físicas identificadas o identificables". Si consultamos la norma (UNE) ISO 17799, nos habla de seguridad de la información, y el punto 12.1.4 se refiere a protección de datos de carácter personal y de la intimidad de las personas.

Consideraremos sinónimos ambos términos a estos efectos, salvo las diferencias que puedan haber establecido la LOPD, el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal u otras normas vigentes o futuras. Creemos que en este contexto se debe hablar de seguridad de los datos (artículo 9 de la LOPD) y de la información (ISO 17799), y ya tratados en conjunto, frente a otras expresiones válidas: seguridad informática, seguridad de las comunicaciones, de las TIC como tecnologías de la Información y de las Comunicaciones.

La clasificación por lo general la entendemos relacionada con la confidencialidad y la integridad, incluso de forma conjunta, si bien en muchos casos hemos de diferenciar, así todos podrán ver la Web de una entidad (salvo posibles áreas reservadas a empleados Intranet, o a distribuidores u otros, Extranet, o bien accesible sólo por clientes o suscriptores), pero muy pocos podrán variar su contenido, es decir, en este caso diferenciamos confidencialidad al leer frente a integridad, posibilidad de modificación de contenidos (Del Peso et al, 2004).

Si nos centramos en la clasificación más común de los datos relacionada con confidencialidad e integridad, algunos posibles niveles pueden ser: de uso interno, de uso restringido, confidencial, secreto o incluso alto secreto.

Tecnologías para la seguridad de la información

Hoy en día, se cuenta con tecnología para la seguridad de la información que cumple con los requerimientos de la LOPD y el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal para el tratamiento de datos personales en el ámbito sanitario como software y sistemas seguros; para la eliminación de vulnerabilidades cortafuegos y proxies; redundancia, que en el caso de un fallo puede tardar minutos en reponer el servicio; los back up para recuperar la información; el control de accesos lógico y físico, que da la capacidad de controlar y conocer quién y cuándo accede a cierta información, a un mensaje o a un servicio, los directorios como LDAP son la clave de cualquier sistema de control de accesos en entornos medianos y grandes; la autenticación que consiste en la comprobación de la identidad del actor; la utilización de *logs* en aplicaciones, sistemas operativos y elementos red para registrar el uso que se hace de ellos y los posibles errores en el sistema; el cifrado, la técnica de seguridad más popular, que convierte a un mensaje en inteligible y se necesitará una clave para descifrar el mensaje (firma electrónica); la reserva que consiste en almacenar suficiente cantidad de un suministro para soportar la interrupción de éste durante un tiempo razonable; y el control de calidad para evaluar la efectividad del centro o servicio sanitario en el mantenimiento y mejora de seguridad (auditoría informática) (Martínez y Rojas, 2014).

Firma electrónica

La firma electrónica o digital en España está regulada por la Ley 59/2003, de 19 de diciembre, es otro de los mecanismos que van a garantizar la seguridad de la información, porque reúne cuatro características particulares autenticación (la identidad de quien ha escrito el mensaje), integridad (que el mensaje no ha sido modificado), no repudio (la persona que envía el mensaje no puede negar el envío) y confidencialidad (que la información no puede ser conocida por otros).

La firma electrónica consiste básicamente en la aplicación de cifrado (algoritmos de encriptación a los datos) de esta forma, el mensaje sólo será reconocido por el destinatario, que podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autenticación, preservando al mismo tiempo la confidencialidad. Para certificar que esta firma electrónica pertenece a determinada persona se encuentra el prestador de servicios de certificación (tercero de confianza) para lo cual emitirá un certificado electrónico o digital incorporado a la firma (Rodríguez, 2004).

Auditoría informática

El artículo 92 del Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (R.D. 1720/2007) se refiere a la auditoría informática, estableciendo que los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

La auditoría examina evidencias, si se producen incumplimientos de las medidas y prácticas de seguridad detalladas en la normativa de seguridad. La clave de una auditoría sea interna o externa es la independencia, la evaluación se debe hacer contra algún patrón, en este caso será contra el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, aunque está teniendo una influencia importante en las implantaciones de seguridad, así como en las revisiones la Norma ISO/IEC 17799 y su versión UNE equivalente en español.

Existen diferencias entre auditoría e inspección, la auditoría que exige el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal frente a la inspección que puede realizar una de las Agencias de Protección de Datos. Las auditorías no se declaran o registran en la Agencia de Protección de Datos al igual que el Documento de Seguridad, pero deben quedar a disposición de la misma.

Consideramos que se debe utilizar la auditoría informática cómo una herramienta para la protección de la información, en este caso para el adecuado tratamiento de los datos de salud contenidos en las bases de datos y sistemas de información de los centros y servicios sanitarios públicos.

Sistema de Gestión de la Seguridad de la Información (SGSI)

En los últimos años ha crecido considerablemente la concienciación y el interés hacia los temas relacionados con la seguridad de los sistemas y tecnologías de la información. Esto viene motivado básicamente por dos razones: por un lado, por la amplia repercusión que están teniendo en los medios de comunicación los últimos incidentes en materia de seguridad y, por otro, por la dependencia cada vez mayor que tienen las organizaciones respecto a los sistemas de información para el correcto desarrollo de sus actividades.

A raíz de esto, se hace necesario homogeneizar de algún modo todos los aspectos relativos a la seguridad de la información por lo que los organismos internacionales responsables han ido desarrollando numerosas normas, entre las que tenemos que destacar la PNE - 150/IEC 27002 y la UNE – 150/IEC 27001:2007. La UNE – 150/IEC 27001:2007 “Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI)”, especifica los requisitos para establecer, implantar, documentar y evaluar un SGSI

dentro del contexto de la organización, con independencia de su tipo, tamaño o área de actividad.

Una herramienta para llevar a cabo las políticas y objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.) por los centros y servicios sanitarios para el tratamiento de datos de salud es contar con un Sistema de Gestión de la Seguridad de la Información (SGSI). El problema es que pocas organizaciones hoy en día cuentan con este grado de seguridad, pero es el inicio, el sector sanitario no debe descartar su implantación por las garantías de seguridad que ofrece.

Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal

Sobre el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de los ficheros físicos y automatizados que contengan datos de carácter personal aprobado por el Real Decreto 17/2007 de fecha 21 de diciembre, podemos decir que tiene como objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamientos, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos personales.

En este Reglamento se establecen tres niveles de medidas de seguridad: básico, medio y alto, siendo correspondientes las medidas de nivel alto para los ficheros que contengan datos de salud. Para poder implantar estas medidas, especialmente las organizativas, y que sean conocidas por las personas que intervengan en el tratamiento, tienen que estar escritas y el Reglamento obliga a que estén recogidas en un Documento de Seguridad (Artículo 88), el mismo que es de obligado cumplimiento para los centros y servicios sanitarios. Este Documento debe identificar al responsable del fichero, el encargado del tratamiento y al o los responsables de seguridad.

La redacción de los artículos 14.4 y 17.6 de la Ley 41/2002 Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica de España da lugar a una interpretación por parte de la Agencia Española de Protección de Datos, confirmando la obligatoriedad de la aplicación del Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal para los centros y servicios sanitarios públicos y privados, sin perjuicio de que la definición y puesta en práctica de las medidas se coordine con las autoridades sanitarias de las Comunidades Autónomas, siempre con respeto al marco previsto en el Reglamento.

La seguridad en la historia clínica electrónica

La introducción de las tecnologías de la información y comunicaciones (TIC) en los centros y servicios sanitarios ha venido condicionada por necesidades generales como las de controlar el gasto, satisfacer a la población

ante la demanda y gestionar los cambios. Se inició con algunos equipos de diagnóstico médicos y de los servicios de gestión económico-financiera, aplicaciones para los servicios clínico-administrativos (gestión de camas, cita previa de consultas externas, o gestión del archivo de historias clínicas), a estas aplicaciones siguieron los programas de codificación de los sistemas de clasificación de pacientes.

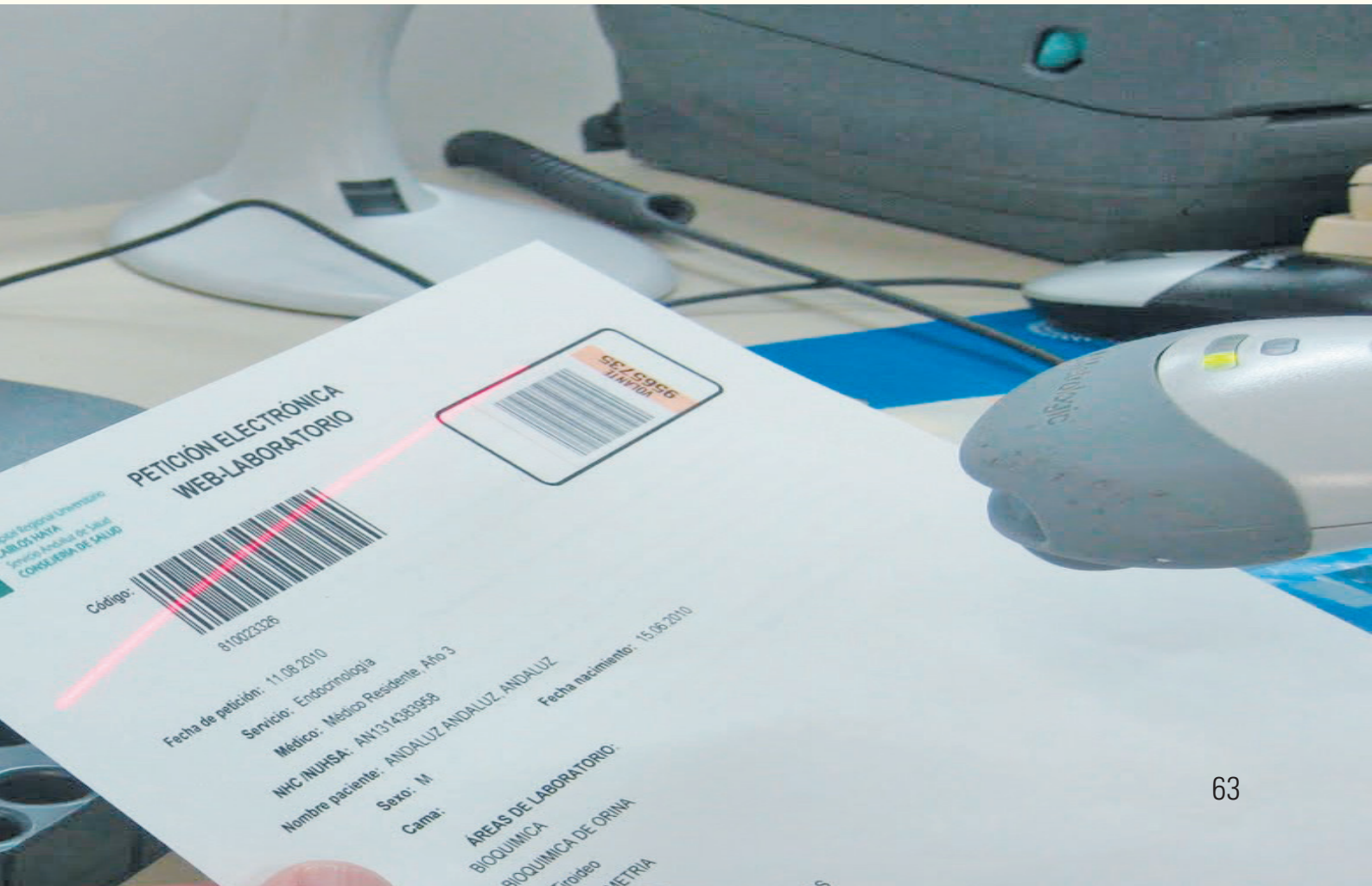
Como establece Carnicero Giménez (2004:272) el concepto de historia clínica cambia con la informatización "de ser un registro del proceso o procesos de un paciente vinculado a un profesional o a un centro sanitario, pasa a ser un registro de todos los antecedentes de salud de una persona que forma parte de un sistema integrado de información".

La historia clínica electrónica tiene como características que es completa; integra todos los episodios asistenciales del paciente no importa dónde y cuándo se hayan producido; es interoperable con otros sistemas como los departamentales, los clínico-administrativos, de gestión económico-financiera y de gestión del conocimiento; accesible en cualquier momento y lugar en que sea necesaria para atender al paciente con las limitaciones debidas a la legislación de protección de datos; flexible permite su utilización a los investigadores, planificadores y evaluadores de la calidad de los servicios entre otros; segura y confidencial; todos los accesos a la historia deben ser registrados y debe identificarse quién accede y qué información introduce o modifica.

Una historia clínica en papel (clásica) ofrece estas dificultades: desorden y falta de uniformidad de documentos; información ilegible; la información se puede alterar; disponibilidad por no estar en el centro sanitario; errores en el archivo; poca garantía de confidencialidad a pesar del control riguroso por parte del responsable de la misma; deterioro del soporte por accidentes (agua y fuego); dificultad de separar los datos de filiación de los clínicos, entre otros.

Es frecuente el acceso a la historia clínica electrónica de un paciente por diferentes departamentos de un mismo centro y por distintos profesionales, con distintas necesidades, por ello el sistema informático deberá atribuir perfiles (médico, especialista, fisioterapeuta, enfermera de planta, técnico de laboratorio, administrativa, etc.) y diseñar la historia de forma que las personas puedan acceder a los apartados que sean necesarios para la función asistencial que desempeñan y se impida el acceso a aquellas partes de la historia clínica respecto de las que no estén autorizados. La historia clínica electrónica permite hacer frente a estas cuestiones de una forma más eficaz que la historia en papel (Instituto de Información Sanitaria, 2009).

La clave para mantener la seguridad y confidencialidad de los datos de salud está en establecer perfiles de usuario, la utilización inapropiada de la autorización para acceder a determinada información está fuera del alcance de las TIC, dependerá de las personas, de los profesionales sanitarios. El sistema de información debe otorgar



las medidas de seguridad adecuadas para que personas extrañas al ámbito sanitario puedan acceder a las historias clínicas. Las razones de interés para acceder a este tipo de información pueden ser variadas, consideramos que una de las principales es la económica.

Hoy en día es una necesidad la implantación de la historia clínica electrónica, porque cada vez más las personas se mueven de un lugar a otro, a lo largo de su vida es vista por diferentes profesionales, a consecuencia de ello tiene más de una historia clínica, distribuida en archivos informáticos y en papel en varias localizaciones y con varios números de identificación.

Conclusiones

Para garantizar la seguridad y confidencialidad de la información clínica se debe resolver la visibilidad de la historia clínica electrónica, para lo cual se establecerán protocolos y guías de actuación. El sistema de información permitirá que todos los accesos a la historia queden registrados (utilización de logs), se pueda identificar quién accede, qué información introduce o modifica (firma electrónica), entre otros. Es importante resaltar que se debe llegar a un equilibrio entre seguridad y disponibilidad, un exceso de medidas para garantizar la confidencialidad de los datos puede colapsar los sistemas y comprometer el acceso a la información, de forma que se impida cumplir con la principal función de la historia clínica electrónica, que es la asistencial, y pierda el sentido todo el proceso, no debemos olvidar que el fin último es ofrecer una atención sanitaria con calidad y eficiencia.

Consideramos la historia clínica electrónica más segura y confidencial que la historia clínica en papel, hay mayores medidas de seguridad en los ficheros automatizados si establecen perfiles de usuarios para las vistas (médico, enfermera, personal administrativo), claves de acceso (firma electrónica) y conocemos el rastro de todos los accesos (logs).

Un componente muy importante en el tema de seguridad, además, de las que puedan otorgar las TIC, es el factor humano. Muchas veces se ha dicho que la persona puede ser el mejor guardián y protector de información tan sensible como son los datos de salud, pero también puede constituir la peor amenaza, cuando no aplica la política de seguridad del centro o servicio sanitario o entran en conflicto otros intereses, como puede ser el económico. Es por esta razón, que consideramos que se debe implicar desde la alta dirección hasta cada uno de los participantes del proceso asistencial y el tratamiento de la información, es una de las claves para tener una eficaz gestión de la seguridad y confidencialidad.

Referencias

1. ACEITUNO C., V. (2004), *Seguridad de la Información*. Creaciones Copyright, S.L. España.
2. CARNICERO G., J. (2004): "La Historia Clínica Informatizada", en León S., P. (2004), *La Implantación de los Derechos del Paciente*. Ediciones Universidad de Navarra, S.A. Pamplona.
3. DE MIGUEL S., N. (2002), *Secreto Médico, Confidencialidad e Información Sanitaria*. Marcial Pons Ediciones Jurídicas y Sociales S.A. Madrid.
4. DE MIGUEL S., N. (2004), *Tratamiento de Datos Personales en el Ámbito Sanitario: Intimidad "versus" Interés Público*. Tirant Lo Blanch. Valencia.
5. DEL PESO N., E., RAMOS G., M.A. Y DEL PESO R., M. (2004), *El Documento de Seguridad. Análisis Técnico y Jurídico. Modelo*. Ediciones Díaz de Santos, S.A. Madrid.
6. DEL PESO N., E. (2003), *Servicios de la Sociedad de la Información. Comercio Electrónico y Protección de Datos*. Ediciones Díaz de Santos, S.A. Madrid.
7. INSTITUTO DE INFORMACIÓN SANITARIA (2009). *El Sistema de Historia Clínica Digital del SNS*. Instituto de Información Sanitaria.
8. MARTÍNEZ S., R. Y ROJAS E., D. (2014), Gestión de la seguridad de la información en atención primaria y uso responsable de Internet y de las redes sociales en *Manual de Salud Electrónica para directivos de servicios y sistemas de salud*. Volumen II Aplicaciones de las TIC a la atención primaria de salud elaborado por la Sociedad Española de Informática en Salud (SEIS) y la Comisión Económica para América Latina y el Caribe (CEPAL) [en línea]: http://repositorio.cepal.org/handle/11362/37058 [Consulta: 17/04/2015]
9. RODRÍGUEZ A., A. (2004), *Firma Electrónica y Documento Electrónico*. Consejo General del Notariado. Madrid.
10. SÁNCHEZ-CARO, J. (2004): "Intimidad, Salud y Constitución" en *La Salud como Valor Constitucional y sus Garantías*, Consejería de Sanidad y Consumo de la Comunidad de Madrid [en línea]: http://www.madrid.org/cs/BlobServer?blobcol=urldata&blobtable=MungoBlobs&blobheadervalue1=filename%3Dintimidad.pdf&blobkey=id&blobheadername1=Content-Disposition&blobwhere=1158621445728&blobheader=application%2Fpdf [Consulta: 15/04/2014]
11. SÁNCHEZ-CARO, J. Y ABELLÁN, F. (2004), *Datos de Salud y Datos Genéticos*. Editorial Comares, S.L. Granada.
12. SÁNCHEZ-CARO, J. Y ABELLÁN, F. (2003), *Derechos y Deberes de los Pacientes. Ley 41/2002 de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas.* Editorial Comares, S.L. Granada.
13. SÁNCHEZ C., C. (2000), *La Intimidad y el Secreto Médico*. Ediciones Díaz S.A. Madrid.