tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

155

MEJORA DE LA CALIDAD DEL SERVICIO EN LA e-SANIDAD. PROTECCIÓN DE LOS DATOS SANITARIOS DE LOS CIUDADANOS

Mar Martínez Sánchez
Business Development Manager
Sector Público
Grupo SIA

Mar Martínez Sánchez

Palabras clave

Servicios, pacientes, derechos, Administración, seguridad, protección de datos, autonomía del paciente, Sanidad, intimidad, consentimiento, confidencialidad, cesión, auditoría, cooperación, descentralización, investigación, movilidad.

Resumen de su Comunicación

La incorporación de las TIC en el entorno sanitario favorecen la universalidad y la equidad en el acceso a la asistencia sanitaria, mejora la atención continua del paciente y amplía la eficacia de los recursos disponibles lo que permite nuevos modelos de relación entre pacientes y organizaciones sanitarias. El tratamiento de datos personales en el ámbito sanitario, exige el cumplimiento de unas garantías que permita afirmar que los datos de salud de los ciudadanos están protegidos y cumplen el marco jurídico que la normativa europea y española establece.

Asimismo, los poderes públicos deberán garantizar a todos los ciudadanos que los datos especialmente protegidos que tratan las AA.PP., únicamente se utilicen y cedan para aquellos fines para los que fueron recogidos y dentro de las previsiones que las leyes sanitarias establecen, garantizando que los SI cumplen con todas las medidas de seguridad establecidas en la LOPD y en el RD 994/97 en el que se establecen las medidas de seguridad que deben cumplir los sistemas que contengan datos personales, con el fin de evitar la lesión de derechos fundamentales.

La tecnología debe ayudar a garantizar la intimidad de los datos personales sanitarios en todo el ciclo de vida desde su obtención, tratamiento, archivo, custodia y transmisión de la información y la documentación clínica. En este sentido, la organización sanitaria garantizará que sus SI se desarrollan y explotan con las medidas de seguridad y pautas de conducta que permitan garantizar el cumplimiento de las obligaciones en materia de información y documentación clínica, que debe asegurarse en condiciones de respeto a la intimidad personal y a la libertad individual del usuario, garantizando la confidencialidad de sus datos personales.

Mar Martínez Sánchez

MEJORA DE LA CALIDAD DEL SERVICIO EN LA ESANIDAD

1. Introducción

Las Administraciones Públicas han sido conscientes de la importancia de las Tecnologías de la Información para mejorar la calidad del servicio, el acceso al mismo con las miras puestas en los pacientes y en el tratamiento de la información. Por este motivo, es esencial fomentar el desarrollo de nuevos servicios, aplicaciones informáticas y herramientas de gestión, dirigidos al sector de la Sanidad, que permitan mejorar su eficiencia en la prestación de servicios a los ciudadanos y faciliten el acceso de éstos a la información y a los servicios interactivos relacionados con la Salud a través de Internet.

Dentro del ámbito de la administración y más concretamente en el área de Sanidad es de gran valor, tanto para los ciudadanos como para los profesionales, la capacidad de acceder a la información en cualquier momento y situación, de tal manera que el Sistema Nacional de Salud (SNS) pueda ofrecer en cada situación y momento la máxima calidad en su atención al paciente. Las ventajas que permiten la interoperabilidad de los sistemas, el uso de la tarjetas sanitaria electrónica, la gestión automatizada en la derivación de pacientes, la futura receta electrónica e intercambio de información de referencias de historias clínicas, entre otros avances, reporta en un beneficio directo para todos los implicados en la Sanidad.

Atención especial requiere la seguridad. El paso firme con el que se persigue este objetivo se encuentra también con nuevos riesgos, inherentes a los nuevos canales de comunicación, a las herramientas informáticas utilizadas y a su uso malintencionado. Estos riesgos deben ser analizados y prevenidos adecuadamente ya que pueden causar graves trastornos y daños en las organizaciones. En este sentido, y paralelamente al desarrollo de la administración electrónica, han surgido un número muy importante de leyes, estándares y recomendaciones de seguridad que consideran las prácticas aplicadas a los procesos de desarrollo, gestión de los sistemas de información, incluyendo el control de los datos objeto de tratamiento.

Claramente la sociedad plantea nuevas demandas que deben de tratarse desde una perspectiva más amplia. No se solicita un cambio de la cobertura sanitaria del ciudadano sino que se esperan nuevos y mejores servicios. Para el funcionamiento real de este pilar básico, se necesita disponer de un soporte de comunicaciones seguro y de suficiente capacidad para abastecer a todo el Sistema Nacional de Salud. En este aspecto, mención especial requiere la Oficina de Seguridad, estructura organizativa específica que se responsabiliza de definir la política de seguridad, garantizar su implantación y la calidad de sus procesos internos, y minimizar los riesgos y las amenazas, anticipándose a ellos.

Por lo tanto, en el desarrollo e implantación de SI en el ámbito de la sanidad será necesario tener en cuenta el cumplimiento del marco jurídico y para ello se recomienda la implantación de medidas tecnológicas de seguridad junto a medidas y políticas de buenas prácticas, todo ello con el fin de garantizar los derechos fundamentales de los ciudadanos en relación con el tratamiento de sus datos personales y el principio de finalidad en el uso de los mismos.

2. Aspectos legales que garantizan el derecho de los ciudadanos en el área de la Sanidad. Protección de datos.

Todo tratamiento de datos personales que se realice entre las distintas AA.PP. debe ser realizado en todo momento al amparo de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), para evitar la lesión de derechos constitucionalmente protegidos. Más concretamente en el terreno sanitario, gran número de organizaciones internacionales, con competencia en la materia, le han dado gran importancia

a los derechos de los pacientes como eje básico de las relaciones clínico-asistenciales: Naciones Unidas, UNESCO, OMS, Unión Europea, etc.

Interés especial requiere el Convenio del Consejo de Europa par la protección de los derechos humanos y la dignidad del ser humano respecto a las aplicaciones de la Biología y la Medicina como primer instrumento internacional con carácter jurídico vinculante para los países que lo suscriben, incluido España. El documento reconoce los derechos de los pacientes destacando el derecho a la información, consentimiento informado e intimidad de la información relativa a la salud de las personas. En esta línea, hay que destacar: Ley 41/2002, de 14 de noviembre, Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que resalta la importancia que tienen los derechos de los pacientes y garantiza la confidencialidad de la información relacionada con los Servicios Sanitarios y el deber de asegurar en condiciones de máximo respeto la intimidad personal y a la libertad individual del usuario; Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que considera los datos relativos a la salud de los ciudadanos como datos especialmente protegidos y establece un régimen riguroso en lo relativo a las medidas de seguridad que deben reunir los ficheros y tratamientos de estos datos; y el Real Decreto 994/199 de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad resaltando la obligación de que los sistemas de información contengan medidas que garanticen la confidencialidad, integridad y disponibilidad de los datos personales, pudiendo acceder a los datos únicamente aquellas personas autorizadas por razón de las funciones que ejerzan o tengan asignadas.

El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso. Únicamente se habilitará el acceso a la historia clínica para los siguientes fines y funciones:

1. Fines de prestación de asistencia sanitaria, diagnostico o de tratamiento (profesionales asistenciales).

2. Fines de administración y gestión de los centros sanitarios (personal con competencias exclusivamente a los datos necesarios para realizar sus funciones).

3. Fines comprobación calidad asistencia, respecto derecho paciente, resto de obligaciones del centro con respecto al paciente o la propia Administración sanitaria (funciones inspección, evaluación, acreditación y planificación (personal sanitario debidamente acreditado con funciones de inspección, evaluación, acreditación y planificación).

4. Fines judiciales (jueces y fiscales).

5. Fines epidemiológicos (las administraciones con competencia en la materia Art. 21 LOPD.

6. Fines salud pública (la administración pública con competencias en la materia)

7. Fines investigación clínica (las entidades con legitimización para realizar investigación clínica).

8. Fines de docencia.

Para los fines descritos en los puntos 5, 6, 7 y 8, el acceso a la historia clínica obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que quede asegurado el anonimato. Únicamente se podría acceder a los datos sin separación cuando el paciente hubiera otorgado su consentimiento.

Bajo este contexto, la cesión de datos puede ser llevada a cabo dentro de la Administración a través de dos vías claramente diferenciadas en nuestro ordenamiento jurídico: comunicación de datos (bajo los requisitos de la obtención del consentimiento previo del afectado o cuando así lo establezca una disposición con rango de Ley y existencia de fines directamente relacionados con las funciones legitimas del cedente y del cesionario, en concordancia con el principio de calidad de los datos descrito en el artículo 5 LOPD); y el acceso a los datos por cuenta de terceros (posibilidad de ceder los datos a un tercero para la prestación de un servicio, que deberá encontrarse reglado a través de un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido).

2.1 Código de Buenas Prácticas para usuarios de sistemas informáticos

La necesidad de garantizar el uso adecuado de las Tecnologías de la Información que la Administración Pública pone a disposición de los responsables de ficheros y tratamientos, hace necesario establecer unas medidas de seguridad y pautas de conducta con el objetivo de facilitar a las personas con acceso a los datos de carácter personal el conocimiento de la aplicación de las mismas en el desarrollo de sus funciones.

Si bien la propia tecnología constituye una herramienta para garantizar la seguridad de la información, también son necesarias medidas de índole organizativa y pautas de conducta que ayuden a concienciar a los usuarios en el uso de las medidas destinadas a aumentar la seguridad.

En este sentido, un Código de Conducta tiene por objeto recopilar los principales aspectos y normas que se deben conocer y aplicar para que todos los usuarios sean conscientes de la necesidad de mantener un nivel de seguridad adecuado en todos los sistemas de información que tengan que utilizar en el desempeño de sus funciones en el ámbito de las competencias de su entidad, sin perjuicio del cumplimiento del resto de las obligaciones que les pudiera ser de aplicación. Además, el Código de Conducta permitirá, que los usuarios conozcan sus obligaciones en relación con el uso de los datos personales y concienciarles de la necesidad de establecer normas y reglas claras que eviten determinadas prácticas y ayuden a garantizar los derechos fundamentales de los pacientes en relación con el uso de sus datos personales. Asimismo, incidirá en el correcto uso de los medios y sistemas de información consecuencia de la necesidad de optimizar la utilización de dichos medios, y de evitar los efectos de un uso inadecuado.

2.2 Plan de Auditorías

El Real Decreto 994/99, de 11 de Junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (Reglamento Seguridad), desarrolla el precepto de la LOPD relativo a las medidas de seguridad y establece las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos, los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervienen en los tratamientos, sujetos al régimen de aplicación de la LOPD

A su vez, establece en su artículo 17 la obligación de realizar auditorías cada dos años de los sistemas de información cuya tipología de información sea de nivel medio o alto.

Una herramienta que automatice el desarrollo y la distribución de los distintos aspectos de la auditoría en relación a las responsabilidades, implicaría poder gestionar la generación de informes (requisito que se recoge en el art.17 del Real Decreto 994/99) desde las distintas unidades funcionales y permitiría impulsar y fusionar los distintos resultados para obtener las evidencias y resultados de forma concurrente y paralela. Igualmente, dicha herramienta, permitiría la generación de cuadros de mando con indicadores representativos del nivel de cumplimiento, además de aprovechar los esfuerzos de la primera implantación en las siguientes auditorías, permitiendo un objetivo constante de mejora y adecuación de LOPD optimizando el esfuerzo.

La herramienta deberá disponer de una arquitectura centralizada a la que acceden las distintas entidades de una misma organización, por lo que se requiere la conectividad de los distintos centros y organismos adscritos (acceso a la herramienta vía Intranet o vía Internet incrementando los mecanismos de autenticación y cifrado en comunicaciones); mecanismos de autorización robustos para evitar accesos a información no permitida de otras entidades, ya que se utilizaría un repositorio común para todas las auditorias de diferentes responsables de ficheros de una misma organización, cifrado del repositorio de datos dinámicos ya que alberga información muy sensible; definición los roles y perfiles por responsable de fichero con las tareas asociadas (responsable de seguridad, su interoperabilidad y segregación de funciones para acometer la auditoria interna).

3. Oficina de Seguridad

Para la implementación y operación del Sistema de Gestión de la seguridad se están constituyendo servicios que se vienen denominando Oficina de Seguridad, estructura organizativa específica que se responsabiliza del diseño, implantación, seguimiento y mejora del SGSI (Sistema de Gestión de Seguridad).

Entre las funciones principales de una Oficina de Seguridad destacan; seguridad preventiva (actividades dedicadas a la implantación de soluciones de seguridad tanto tecnológica como organizativa); seguridad reactiva (gestión de incidentes de seguridad para su solución con el menor impacto en la organización); y seguridad consultiva (asesoría continua de seguridad de los sistemas de información).

Estas funciones tratan de manera horizontal los principales aspectos de seguridad con el fin de incrementar el nivel de seguridad de los sistemas de información de una entidad pública o privada, tanto en las comunicaciones como en los sistemas, en una adecuación legal, en la continuidad de negocio y la normalización y concienciación.

La Oficina de Seguridad deberá responder ante la Dirección de las organizaciones, responsables finales de la seguridad. Recordemos que el Real Decreto 994/1999, de 11 de junio, establece la obligación de los responsables de ficheros, y, en su caso, encargados de tratamiento, que deberán adoptar las medidas de índole técnica y organizativa en los sistemas de información que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos. Es decir, que únicamente podrán tratarse datos personales en su SI que reúnan las condiciones de seguridad que se determine por el reglamento de seguridad. Esta previsión es especialmente importante en el acceso a los datos especialmente protegidos de los sistemas sanitarios debido al alto grado de sensibilidad que contendrá la información registrada. Sin embargo, también se da la doble circunstancia, de la necesidad de una alta disponibilidad de los datos ante situaciones de urgencia médica, así como la necesidad de acceso a los mismos en diversas circunstancias y en distintos servicios y zonas de un hospital o centro de atención sanitaria.

4. Cooperación entre las diferentes Administraciones Públicas en términos sanitarios

Con la transferencia de competencias en materia sanitaria, del Sistema Nacional de Salud, en los últimos años, las Comunidades Autónomas también están llevando a cabo distintas medidas para la modernización e impulso del Gobierno Electrónico en el área de Sanidad, orientadas a impulsar el desarrollo de servicios para los ciudadanos, a facilitar el intercambio de información entre administraciones y apoyar la reorganización interna de procesos de los centros de atención especializada y atención primaria.

Las estrategias de salud pública basadas en infraestructuras tecnológicas y aplicaciones e-salud permiten a los poderes públicos centrar toda su gestión alrededor del paciente y contribuir a mejorar la calidad asistencial y los ratios servicios/coste/eficiencia.

El Plan de Acción eEurope 2005 prevé el desarrollo de sistemas de interoperabilidad, fomentar el trabajo en red entre organizaciones (Colegios profesionales de farmacéuticos, médicos, enfermería, redes nacionales de salud, europeas e internacionales como las de transplantes, epidemiológicas, investigación tumores, etc).

Los Sistema de Información Sanitaria deben gestionar de una forma global los servicios prestados en los Centros de Atención Primaria y especializada que garantice todas la previsiones que las leyes establecen en materia de seguridad y protección de datos sanitarios, garantizando (pacientes, familiares, personal sanitario, no sanitario y dirección) que se cumplen con los principios de la Recomendación Nº R (97) 5, Directiva 95/46/CE; adecuación LOPD; adecuación a la Ley Autonomía del Paciente; y confidencialidad, integridad y disponibilidad.

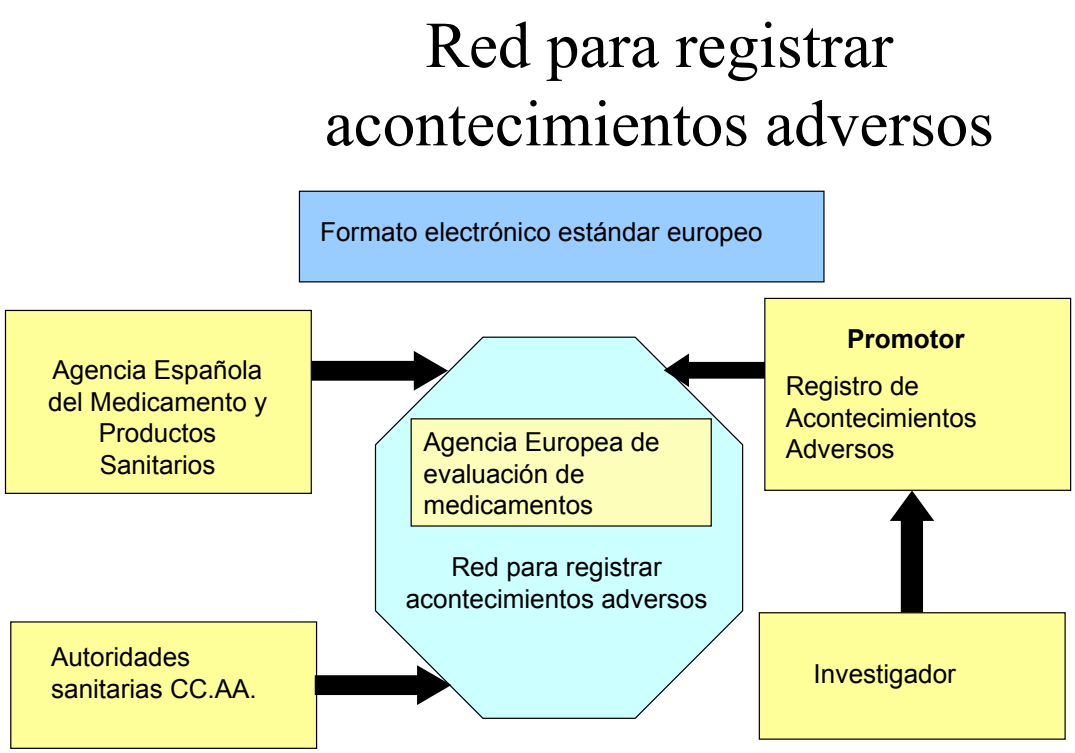
Dentro del marco jurídico nos encontramos con la Ley 41/2002 de Autonomía del Paciente y Derechos y Obligaciones en materia de Documentación Clínica, que afecta a todas las Comunidades Autónomas. Entre los principales artículos destacan: Artículo 14.2 (cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información), Artículo 14.3 (las Administraciones sanitarias establecerán los mecanismos que garanticen la posibilidad de reproducción futura entre otros), Artículo 14.4 (las CC.AA. aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias y evitar su destrucción y pérdida accidental).

4.1 Casos prácticos de Cooperación: Utilización de Datos para Estudios e Investigación Científica

El régimen jurídico a que se somete la realización de los ensayos clínicos trata de garantizar el respeto de los derechos humanos y la dignidad de la persona respecto a la aplicación de la biología y la medicina reflejados en la Declaración de Helsinki y en el Convenio de Oviedo. Así lo señala en su preámbulo. A tal efecto exige el dictamen favorable del Comité Ético de Investigación Clínica –que realizará un seguimiento del ensayo hasta su recepción final- (arts.15 y 10 del Decreto 223/2004), autorización de la Agencia Española de Medicamentos y productos sanitarios (arts.20 a 23, Decreto 223/2004) y realizase de acuerdo con las normas de buena práctica clínica (art. 34, Decreto 223/2004), imponiéndose a los investigadores unas normas severas de vigilancia de la seguridad (arts.42 a 47).

Este avance permitirá que se obtenga y se documente el consentimiento informado de cada uno de los sujetos del ensayo, libremente expresado y deberá estar documentado (hoja de información para el interesado y documento de consentimiento). El tratamiento, comunicación y cesión de los datos de carácter personal de los sujetos participantes en el ensayo se ajustarán a lo dispuesto en la LOPD y constará expresamente en el consentimiento informado. Paralelamente, los sujetos del ensayo dispondrán de un punto donde puedan obtener mayor información (dirección a través de la cual podrán ejercitar los derechos de acceso, oposición, rectificación y cancelación).

Como punto importante está la creación de la EudraCT, base de datos de Ensayos Clínicos para la Unión Europea, que según la Directiva 2001/20/EC del Parlamento Europeo y del Consejo, de 4 de abril de 2001 (relativa a la aproximación de las disposiciones legales reglamentarias y administrativas de los Estados miembros sobre la aplicación de buenas prácticas clínicas en la realización de ensayos clínicos de medicamentos de uso humano), deberá contener información sobre todos los ensayos clínicos en los que se incluya al menos un centro ubicado en un Estado Miembro de la Comunidad. Esta base de datos deberá contener una parte de la información requerida en el formulario de solicitud europeo de ensayo clínico, datos sobre la situación de autorización o no del ensayo en cada uno de los Estados involucrados en el mismo, incluyendo una referencia a la opinión del Comité Ético correspondiente, identificación de las modificaciones relevantes, la declaración de final del ensayo, y una referencia a las sobre cumplimiento de las Normas de Buena Práctica Clínica realizadas.



5. El reto de la tecnología móvil en favor del paciente

La aplicación de la movilidad en la Sanidad es ya una realidad. La plataforma móvil de servicios en Hospitales y Centros de Atención primaria empiezan a ser una realidad y sirven como ejemplo de las ventajas que reportan estas tecnologías en el ámbito sanitario. La utilización de esta plataforma telemática tiene muchas funcionalidades, se pueden remarcar como ejemplo los sistemas que recuerda a sus pacientes, vía mensaje al teléfono móvil (sms), las citas con el médico, lo que supondrá una reducción en las citas fallidas o del absentismo, fenómeno que perjudica a las listas de espera. Este tipo de proyecto podrá disminuir la tasa de pacientes no presentados a consultas en porcentajes muy reseñables.

Otra tipo de funcionalidad es aquella que ha proporcionado al personal sanitario de PDAs disponiendo de la información de los pacientes que necesitan cuando están realizando la visita. Dentro del hospital utilizan conectividad WI-FI, y en las visitas a domicilio se emplea GPRS.

También se está utilizando este tipo de tecnología, para recordar a un paciente las horas y tomas de un medicamento.

Todos estos avances y los que están por llegar dejan visibles las enormes potencialidades que nos ofrece las aplicaciones móviles para mejorar la relación del sistema sanitario con los ciudadanos, en aspectos como recordarles sus citas médicas, el calendario vacunal de sus hijos, lanzamiento de consejos sanitarios o información relativa a su medicación.