Sociedad Española de Informática y Salud · Nº 94· Septiembre 2012

I+S

INFORMATICA Y SALUD

Monográfico: La protección de datos personales

Entrevistas a Santiago Abascal, Esther Mitjans e Iñaki Pariente

I Seminario de Protección de Datos en Atención Sociosanitaria

IX Foro sobre Protección de Datos

Entidades Asociadas

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

accenture
Alto rendimiento. Hecho realidad.

APD

Bilbomática

Carestream

CITRIX

CSC

Engisys
Engisys Solutions

FUJITSU

gmv

Ibermática
Tecnología y Conocimiento

InterSystems

iic
instituto
de ingeniería
del conocimiento

mHealth Alert

NUANCE

orange

ORION HEALTH

QMATIC
Valuing Time

satec

sigesa
Case-Mix Knowledge

steria

Tecnocom

Telefónica

UDIAT
Centre Diagnòstic

Vademecum

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Director
Salvador Arribas

Comité editorial
Luciano Sáez
Marcial García Rojo
Rosa Valenzuela
Elvira Alonso
José Luis Carrasco

Consejo de Redacción
Rodrigo García Azurmendi
Miguel Chavarría
Fernando Bezares
José Quintela
Alberto Gómez Lafón
Jesús Galván
María Rovira
Julio Moreno
José Luis Monteagudo
Cristina Cuevas
Begoña Otalora
Emilio Aced
Fernando Escolar
Carlos García Codina
Vicente Hernandez
Carlos Hernández
Juan Fernando Muñoz
Juan Manuel de León
Carlos Parra
Antonio Poncel
Francisco Javier Francisco Verdú
Carlos Royo
José Lagarto
Isabel Aponte
Guillermo Vázquez
Javier Carnicero

Colaborador Técnico
Diego Sáez

Información, Publicidad, Suscripciones y DISTRIBUCIÓN:
CEFIC. C/ Enrique Larreta, 5 Bajo Izda
28036 Madrid
Tlfno: 913 889 478 • Fax: 913 889 479
e-mail: cefic@cefic.es

Producción Editorial:
Tel. 902 271 902 • Fax: 902 371 902
E-mail: mic@editorialmic.com
www.editorialmic.com
Editorial MIC

DL: M-12746-1992
ISSN: 1579-8070

Año 2012. Sumario nº 94

Editorial 5

MONOGRÁFICO
LA PROTECCIÓN DE DATOS PERSONALES

- Introducción 7
- ¿Atención sociosanitaria vs. protección de datos de carácter personal? 9
- El tratamiento de datos de salud conforme al Proyecto de Reglamento Europeo de Protección de Datos 12
- La protección de datos en el día a día de un gerente en un hospital ¿misión imposible? 15
- Una introducción al impacto del "cloud computing" 20
- Seguridad, protección de datos y responsabilidad en Cloud Computing 23
- Dudas y soluciones en relación con algunas cuestiones recurrentes en protección de datos de salud 25
- Protección de datos de salud: casos prácticos de la experiencia de la Autoridad Catalana de Protección de Datos 28
- La mejora de la información clínica: una garantía para la seguridad del paciente 30
- La seguridad, las estrategias y la ortografía 33
- SEGURIDAD: Beneficios 360º 36
- Ética en la creación y gestión de biobancos: problemas y soluciones en red 38

Entrevista a Esther Mitjans Perelló
- Directora de la Autoridad Catalana de Protección de Datos 42

Entrevista a Iñaki Pariente de Prada
- Director de la Agencia Vasca de Protección de Datos 44

Entrevista a Santiago Abascal Conde
- Director de la Agencia de Protección de Datos de la Comunidad de Madrid 48

ACTIVIDADES DE LA SEIS
- I SEMINARIO DE PROTECCIÓN DE DATOS EN LA ATENCIÓN SOCIOSANITARIA 51
- IX FORO SOBRE PROTECCIÓN DE DATOS 53

SOCIOS TECNOLÓGICOS

InterSystems · CSC · Microsoft · Telefónica

COLABORADORES TECNOLÓGICOS

AGFA HealthCare · Atos · Citrix · EMC² · intel · Fujitsu · Informática El Corte Inglés · Oracle · T-Systems · UNIT4

Los artículos revisiones y cartas publicadas en I+S, representan la opinión de los autores y no reflejan la de la Sociedad Española de Informática de la Salud

Entidades Colaboradoras

- AGÉNCIA CATALANA DE PROTECCIÓN DE DADES
- AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID
- AGFA
- ATOS ORIGIN
- COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES
- COLEGIO OFICIAL DE FARMACÉUTIOS DE BADAJOZ
- CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS
- CSC
- EMC
- EMEDICA,S.L.
- EMERGRAF, S.L. CREACIONES GRÁFICAS
- EMPRESA PÚBLICA HOSPITAL ALTO GUADALQUIVIR
- EVERIS
- FUJITSU
- HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN
- HOSPITAL GENERAL DE LA PALMA
- HOSPITAL GENERAL GREGORIO MARAÑÓN
- HOSPITAL LLUÍS ALCANYÍS DE XÁTIVA
- INFORMÁTICA EL CORTE INGLÉS
- INSTITUTO DE SALUD CARLOS III
- INTEL
- INTERSYSTEMS
- MICROSOFT
- MUTUA UNIVERSAL
- MUTUAL CYCLOPS-CENTRE DOCUMENTACIÓ
- ORACLE
- OSAKIDETZA - SERVICIO VASCO DE SALUD
- TELEFÓNICA DE ESPAÑA, S.A.
- T-SYSTEMS
- UNIT 4
- VALLPLASA ATENCIO PRIMARIA

Editorial

Las acciones de la Sociedad Española de Informática de la Salud sobre protección de datos y seguridad de la información de salud se inician con la promulgación de la LORTAD en 1992. Nuestra Sociedad vio claramente que la legislación en esta materia afectaba a la implantación de las TIC en nuestro sector y era un elemento positivo de cara a garantizar la confidencialidad, la disponibilidad y seguridad de los datos de salud, convirtiéndose en prerrequisito básico e imprescindible a la hora de diseñar e implantar los sistemas de información de salud.

Sin embargo para cumplir los mandatos legislativos había que hacer otras muchas acciones al margen de las puramente tecnológicas, tales como definición y modificación de procedimientos, roles profesionales y un importante cambio cultural.

Para ello y con el apoyo y la colaboración de la Agencia Española de Protección de Datos y de las tres agencias autonómicas existentes: la Agencia de Protección de Datos de la Comunidad de Madrid, la Agencia Vasca de Protección de Datos y la Agencia Catalana de Protección de Datos (ahora Autoridad Catalana de Protección de Datos); incorporamos sesiones o ponencias sobre protección de datos en las distintas actividades de la Sociedad, se realizan diversas publicaciones tanto en INFORME SEIS como en esta revista y se crea en 2004 el Foro de Protección de Datos de Salud diseñado por su Comité Ejecutivo del que forman parte representantes de las Agencias.

Este Foro nace como resultado de evaluar la situación a través de las actividades realizadas y viendo la necesidad de disponer de una actividad especifica que coordine y defina las acciones requeridas para convertir lo que a priori, pudiera parecer un freno para la implantación de soluciones innovadoras mediante la tecnologías de la información y las comunicaciones, en un elemento impulsor de las mismas.

Buscamos una denominación especial a esta actividad "Foro de protección de datos de salud", no solo con la intención de realizar un seminario y una jornada de trabajo anual, sino que se crea una comunidad de interés para canalizar una opinión y plantear la adopción de medidas encaminadas a impulsar la protección de datos y mantener una línea de comunicación y participación de todos los profesionales interesados, los tecnológicos, los sanitarios, los gestores y las Agencias de Protección de Datos.

Es conocida la complejidad de nuestros sistemas de información y la alta protección que debemos asegurar al tratarse de datos de salud, por ello las medidas a adoptar no solo deben ser tecnológicas y de procedimiento, es preciso impulsar esta cultura de confidencialidad y seguridad de la información a todos los profesionales que intervienen en la protección de la salud.

Uno de los objetivos esenciales de este foro, es transmitir a los directivos del sistema sanitario y a los profesionales de la salud, que la protección de datos es un factor clave para la implantación de las tecnologías de la información y comunicaciones en el ámbito sanitario.

El Foro de Protección de Datos de Salud se ha convertido hoy después de 8 años de funcionamiento en una importante vía de comunicación y de transmisión de conocimientos sobre todos los aspectos que afectan a los sistemas de información de salud y socio sanitarios, a su confidencialidad y seguridad gracias a la apuesta decidida de las Agencias de Protección de Datos y del Gobierno de Navarra ya que este, primero a través de NGA y ac-

Editorial

tualmente de SODENA, nos facilita el soporte necesario para materializarlo.

Los temas que han orientado las reuniones de estos 9 años ha sido:

"El papel del profesional de la salud", "Objetivo: implicar a los profesionales", "La confidencialidad en la Historia de Salud", "La seguridad de la Información requisito para la calidad de la asistencia sanitaria", "Impacto del nuevo Reglamento de la LOPD en el Sistema Sanitario", "La Salud en Red: un reto para la Protección de Datos", "Los derechos de protección de datos de las personas en situaciones difíciles", "Protección de Datos: derecho de las personas y obligación de los profesionales e instituciones " y "La integración de la protección de datos personales en la atención sanitaria" habiéndose revisado en todas ellas aspectos legislativos, éticos, organizativos, de procedimiento y soluciones tecnológicas.

Hoy con este monográfico esperamos ampliar la función difusora de este Foro y que sus ya muchos seguidores aumenten. Por parte de la Sociedad Española de Informática de la Salud pondremos todos nuestros recursos para cumplir sus objetivos y gracias al apoyo y ánimo que las Agencias de Protección de Datos y SODENA nos brindan, afrontamos con ilusión mejorar día a día las actividades del Foro de Protección de Datos de Salud.



La protección de datos personales

Emilio Aced Félez
Subdirector General de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid
Delegado de Protección de Datos de la SEIS y Coordinador del Foro de Protección de Datos de Salud

La protección de datos personales en el ámbito sanitario es un tema crucial y que siempre genera interesantes debates por la tensión existente entre la necesidad de un conocimiento exhaustivo de información de los pacientes (no siempre circunscrita exclusivamente a parámetros relativos a su salud estrictamente entendida) y el imprescindible y obligado respeto a sus derechos como personas y ciudadanos.

Consciente de ello, la SEIS ha querido dedicar de nuevo un número monográfico a esta materia para tratar de suministrar materiales para la reflexión y, en la medida de lo posible, directrices para abordar los problemas con los que se encuentran los profesionales y trabajadores que prestan sus servicios en el sector sanitario.

Los protagonistas de este número, esto es, los autores de los trabajos que en él se contienen, son expertos en distintas áreas conectadas de una u otra manera con la prestación de servicios de salud a los que se les ha pedido que complementaran y elaboraran más exhaustivamente los temas de los que se ocuparon en el IX Foro de Protección de Datos de Salud, celebrado en Pamplona los pasados 25 y 26 de abril.

A todo ellos, mi gratitud y la de la SEIS por haber aceptado realizar el esfuerzo y sacrificar tiempo de descanso para poder ofrecerles una amplia panorámica de temas de máxima actualidad e interés que suscitaron interesantes debates en el Foro. En particular, quiero agradecer a Javier Sempere, compañero en la APDCM, el excelente resumen que ha realizado de las sesiones del Foro y que se incluye en este monográfico. Estoy seguro de que les permitirá a Uds. tener una idea cabal de los temas que allí se trataron y de que les servirá de precisa introducción al resto de los trabajos.

Igualmente, hemos considerado que sería de gran interés para todos nuestros lectores conocer la opinión de los directores de las tres autoridades autonómicas españolas de protección de datos y, por ello, les solicitamos que contestaran una serie de preguntas sobre su visión del presente y el futuro de la protección de datos personales en la sanidad española. Todos ellos accedieron inmediatamente haciendo gala de su tradicional amabilidad y apoyo a las iniciativas de la SEIS.

Por ello, desde la SEIS queremos, una vez más, hacer público nuestro agradecimiento a D. Santiago Abascal, Director de la Agencia de Protección de Datos de la Comunidad de Madrid, a Dña. Esther Mitjans[1], directora de la Autoridad Catalana de Protección de Datos y a D. Iñaki Pariente, director de la Agencia Vasca de Protección de Datos, por compartir con nosotros unas reflexiones que estoy seguro nos ayudarán a todos a entender mejor la actividad y las acciones de las autoridades de control de protección de datos.

El contenido de este número monográfico se ha estructurado en torno a las sesiones del Seminario sobre Protección de Datos en la Atención Sociosanitaria –celebrado como introducción al Foro propiamente dicho en la mañana del día 25 de abril- y del IX Foro de Protección de Datos de Salud para dotar a las mismas de un hilo conductor que pudiera hacer más atractiva y enriquecedora la lectura de las contribuciones de los autores.

Así, el mismo comienza con el análisis de aspec-

[1] *En el momento de cerrar este número el Parlamento de Cataluña había procedido a nombrar nueva Directora de la Autoridad Catalana de Protección de Datos a Dña. M. Àngels Barbarà i Fondevila.*

tos relativos a la interrelación entre los servicios sociales y sanitarios y la problemática derivada del acceso a los datos de salud por parte de los trabajadores sociales, continúa con la forma en que se abordan en el día a día de un centro sanitario los problemas cotidianos y, en particular, el acceso a las historias clínicas para, a continuación, adentrarse en un terreno más tecnológico para presentar los beneficios de la "computación en la nube" así como sus riesgos y la forma de minimizarlos.

Seguidamente, las autoridades de protección de datos introducen una cierta miscelánea para describir los casos más interesantes que han tenido que abordar en el último año y las soluciones aportadas por las mismas para, de nuevo, sin solución de continuidad, revisar aspectos técnicos y organizativos en el ámbito de las medidas de seguridad que deben proteger el tratamiento de datos personales.

Finalmente, el número se cierra de una manera poco usual en esta revista y en este ámbito pero extremadamente interesante: con una reflexión filosófica por parte de Antonio Casado, Profesor del Departamento de Filosofía de los Valores y Antropología Social de la UPV/EHU, sobre las implicaciones éticas en la creación y gestión de biobancos.

Espero que este número les resulte de interés y les ayude a profundizar en el amplio y complejo mundo de la protección de datos de salud y les proporcione apoyo y materiales de reflexión para promover la implantación de nuevas políticas de seguridad y protección de datos en sus entornos profesionales y les proporcione ideas para evolucionar y mejorar las existentes en estos momentos. Si ello es así, habremos cumplido con el objetivo que nos propusimos al confeccionar este número monográfico sobre protección de datos de salud.



¿Atención sociosanitaria vs. protección de datos de carácter personal?

Jordi Ferreres i Jovani
Secretario General Autoridad Catalana de Protección de Datos

Los días 25 y 26 de abril de 2012, organizado por el Gobierno de Navarra, la Sociedad de Desarrollo de Navarra (SODENA) y la Sociedad Española de Informática de la Salud (SEIS), se celebró en Pamplona el IX Foro sobre Protección de Datos de Salud, dedicado a la integración de la protección de los datos personales en la atención sanitaria. La primera jornada, el Foro acogió el Seminario sobre Protección de Datos en la Atención Sociosanitaria, que contó, como ponentes, con representantes de las cuatro entidades de control de protección de datos, entre ellos quien firma estas líneas.

Algunas intervenciones de los asistentes al Seminario dejaron entrever reproches a la regulación de la protección de datos, por no tener en suficiente consideración las especificidades de las tareas (asistenciales o de gestión) encomendadas al personal con responsabilidades en la atención sociosanitaria. Parecería que las exigencias de la Ley orgánica 15/1999, de 13 de diciembre, y del Reglamento que la desarrolla, y los principios en que una y otro se sustentan suponen una complicación, cuando no un obstáculo, para los cometidos de aquellos profesionales. Los comentarios incidían en los problemas derivados de la comunicación de datos especialmente protegidos, sobre todo de salud.

Esta visión de la protección de datos de carácter personal como un elemento que entorpece el quehacer diario no es privativa, por supuesto, de las personas procedentes del ámbito sociosanitario; se ha manifestado en otros foros. El profesional se afana en llevar a cabo su labor y en atender al usuario del servicio de la mejor manera posible. Y en su afán tropieza con unas normas -cuyo incumplimiento lesiona un derecho fundamental- que le dificultan obtener información que, en ocasiones, es indispensable para su tarea. Este artículo se ha preparado a partir de la ponencia del Seminario, referida a los principios de protección de datos.

1. EL PLAN FORAL DE ATENCIÓN SOCIOSANITARIA

¿Cuál es el marco de actuación para los profesionales de la atención sociosanitaria en Navarra? Según el Plan foral, aprobado inicialmente por acuerdo del Gobierno de Navarra de 27 de junio de 2000, el modelo de atención sociosanitaria debe ser:

- Integral: que tenga en cuenta las necesidades de atención (físicas, emocionales, sociales y espirituales) de las personas enfermas y con discapacidad y de sus familias, e
- Interdisciplinar: con participación de los diferentes profesionales que deberán intervenir para prestar una atención integral y continuada, mediante equipos multiprofesionales, que permitan obtener los máximos estándares de calidad y eficacia en la valoración y detección de las necesidades, en la prevención de complicaciones, en la planificación de las actividades y en la evaluación de los resultados obtenidos. La multidisciplinariedad pasa por el acercamiento de los sistemas sanitario y social y la elaboración conjunta de protocolos de actuación, a partir de la comunicación y el intercambio.

El Plan foral fija, como uno de sus objetivos, alcanzar una suficiente coordinación entre el Sistema de Servicios Sociales y el Sistema Sanitario, que garantice la continuidad de los servicios sociosanitarios entre los distintos dispositivos y niveles de atención.

Otras partes del Plan aluden a la interrelación y la coordinación entre servicios sociales y sistema sanitario. Así, el que se dedica a la salud mental; o cuando se define el modelo de organización de recursos; o el programa de gestión de altas hospitalarias, o al tratar de la atención primaria sociosanitaria. En este último caso, por ejemplo, se hace referencia al diseño de un impreso único de recogida de información sanitaria para el acceso a las prestaciones sociales o a la valoración conjunta de los casos por una comisión formada por profesionales del centro de salud y un trabajador social.

El Plan subraya, asimismo, la necesidad de disponer de un sistema de información que recoja datos sanitarios, valoración de capacidad funcional y situación social para definir las necesidades de la persona usuaria.

2. REFERENCIAS A LA PROTECCIÓN DE DATOS EN LA REGULACIÓN DE LA ATENCIÓN A LAS PERSONAS EN SITUACIÓN DE DEPENDENCIA

Entre los principios inspiradores de la Ley 39/2006, de

14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia, están la transversalidad de las políticas de atención a la personas en situación de dependencia, la colaboración de los servicios sociales y sanitarios en la prestación de los servicios a los usuarios y la cooperación interadministrativa. La ley, en el artículo 4.d), reconoce a las personas en situación de dependencia el derecho a que sea respetada la confidencialidad en la recogida y el tratamiento de sus datos, de acuerdo con la Ley orgánica de protección de datos de carácter personal. Y al tratar de la red de comunicaciones, dispone que el uso y la transmisión de la información en esa red estarán sometidos al cumplimiento de lo dispuesto en la mencionada Ley orgánica (artículo 38.2).

Por su parte, la Ley foral 1/2011, de 15 de febrero, por la que se establece el procedimiento para el reconocimiento de la situación de dependencia y se regula la organización, las funciones y el régimen del personal que configura los equipos y el órgano de valoración de la situación de dependencia en Navarra, recoge, entre los deberes del personal valorador en el ejercicio de sus funciones, observar siempre el máximo respeto y consideración, protegiendo especialmente la intimidad de las personas a valorar; guardar secreto y sigilo profesional respecto a los asuntos que conozca por razón de su cargo, funciones y actuaciones; y guardar confidencialidad respecto a los datos personales que afecten o puedan afectar a la intimidad de las personas (artículo 6).

Igualmente, el Reglamento marco de Régimen interno de los servicios residenciales propios y concertados de la Agencia Navarra de Dependencia reconoce a las personas usuarias el derecho a la confidencialidad respecto de la información que sea conocida por el equipo de atención, al acceso, en cualquier momento, a su expediente individual y a que el tratamiento de sus datos personales se realice de acuerdo con la legislación vigente.

3. LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El ordenamiento jurídico español recoge los principios de la protección de datos de carácter personal en la Ley orgánica 15/1999, de 13 de diciembre, reguladora de la protección de datos de carácter personal, y en el Reglamento que la desarrolla, aprobado mediante el Real decreto 1720/2007, de 21 de diciembre.

Los principios -se cita el artículo de la ley orgánica- son:

- calidad de los datos (4)
- derecho de información (5)
- consentimiento del afectado (6)
- existencia de datos especialmente protegidos (7 y 8)
- seguridad de los datos (9)
- deber de secreto (10)
- comunicación o cesión de datos (11) y
- acceso de los datos por cuenta de terceros (12)

Es en base a esos principios que la persona puede decidir cuáles de sus datos facilita a un tercero o cuáles puede el tercero recabar; y son los principios los que le permiten saber quién posee los datos y para qué, pudiendo oponerse a esa posesión o uso. Este poder de control y disposición se concreta jurídicamente en la facultad de consentir sobre la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento por un tercero, así como los usos por este.

Los principios son de obligado cumplimiento desde el momento en que se produce la recogida de datos de la persona afectada o interesada, siempre y cuando sean almacenados en un fichero.

4. ¿ATENCIÓN SOCIOSANITARIA VS. PROTECCIÓN DE DATOS?

Entre las cuestiones planteadas durante el Seminario sobre Protección de Datos en la Atención Sociosanitaria sobresalieron el intercambio de información, entre los servicios de salud y los servicios sociales y con los pacientes; el seguimiento de las actuaciones; el acceso a la información clínica de las personas atendidas en los centros sociales; la consulta de la tramitación administrativa de los expedientes por parte de los trabajadores sociales; el archivo y la custodia de datos, y el acceso a datos personales por parte de la Administración y la negativa del titular a facilitarlos.

El simple enunciado de esas cuestiones ya denota la preocupación generada en quien las plantea. Hemos visto que la normativa sectorial incluye continuas cautelas y remisiones a la protección de datos. Parece, a primera vista, que hay razones para el desaliento de los profesionales.

Pero, si examinamos las normas señaladas anteriormente, vemos que, junto a remisiones a la regulación de la protección de datos y referencias a conceptos como intimidad, confidencialidad o secreto, incluyen medidas e instrumentos destinados a facilitar el trabajo de los profesionales. A título de ejemplo:

La creación de un sistema de información del Sistema para la Autonomía y Atención a la Dependencia, que garantice la disponibilidad de la información y la comunicación recíproca entre las Administraciones Públicas, recogida en el artículo 37 de la Ley 39/2006.

De acuerdo con la misma ley, el Ministerio de Trabajo y Asuntos Sociales ha de poner a disposición del Sis-

tema para la Autonomía y Atención a la Dependencia una red de comunicaciones -ya se ha mencionado- que facilite y dé garantías de protección al intercambio de información entre sus integrantes. A través de la red se intercambiará información sobre las infraestructuras del sistema, la situación, grado y nivel de dependencia de los beneficiarios de las prestaciones, así como cualquier otra derivada de las necesidades de información (artículo 38).

La previsión del artículo 15.2 de la Ley foral 1/2011, según el cual, para la elaboración del Programa Individual de Atención, que debe formalizar la unidad administrativa competente, se atenderá al contenido del informe social emitido por el personal técnico de la Red Pública de Servicios Sociales de Base Municipales, pudiéndose tener en cuenta, igualmente, otros informes técnicos aportados por la persona interesada o por otras entidades públicas que faciliten información necesaria para la elaboración del Programa.

O, finalmente, la posibilidad de petición de los expedientes, iniciados en otras Comunidades o Ciudades Autónomas, de aquellas personas que trasladen su residencia al ámbito territorial de la Comunidad Foral de Navarra a la Administración de origen (disposición adicional tercera).

5. CONCLUSIÓN

Es verdad que la regulación de la protección de datos de carácter personal establece limitaciones al tratamiento de los datos, que los datos de salud gozan de unas garantías reforzadas o que la comunicación de datos solo es posible si se cumplen determinadas condiciones. Pero, siendo todo esto cierto, también lo es que tanto dicha regulación, como las diferentes legislaciones sectoriales (lo hemos comprobado en la sociosanitaria) contemplan excepciones y ofrecen instrumentos para satisfacer los requerimientos derivados de la actividad de los profesionales. Ahí radica la clave del asunto. En conocerlos.



El tratamiento de datos de salud conforme al Proyecto de Reglamento Europeo de Protección de Datos

Ángel Igualada Menor
Subdirector General Adjunto de Registro de Ficheros y Sistemas de Información. Agencia de Protección de Datos de la Comunidad de Madrid

El nuevo Proyecto de Reglamento Europeo de Protección de Datos, con el objetivo de armonizar la aplicación de la normativa vigente en materia de Protección de Datos en todos los países de la Unión, eliminando la inseguridad jurídica producida por las diferencias generadas en la trasposición de la Directiva 95/46/CE por los Estados miembros, va a implicar algunos cambios sustanciales respecto a las obligaciones que deben cumplirse en los tratamientos de datos personales.

De una manera significativa, los cambios van a afectar a los tratamientos de datos de salud y, para conseguir el cumplimiento del nuevo Reglamento será necesario realizar importantes adaptaciones en los tratamientos de datos, aún cuando no podemos obviar que estamos analizando un proyecto de Reglamento, que puede ser objeto de modificación a lo largo de su tramitación hasta su aprobación definitiva y, que éste prevé plazos de adaptación de los tratamientos a los mandatos que contiene.

La primera novedad importante introducida por el proyecto de Reglamento, respecto al tratamiento de los datos de salud, es la modificación de su definición. En este momento, conforme a lo establecido en el Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, se consideran datos de carácter personal relacionados con la salud, "las informaciones concernientes a la salud pasada, presente o futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética". El considerando 26 del proyecto de Reglamento Europeo establece que "los datos personales relacionados con la salud deben incluir en particular todos los ratos relativos a la salud del interesado; información sobre el registro de la persona para la prestación de servicios sanitarios; información acerca de los pagos o de la admisibilidad para la atención sanitaria con respecto a la persona; un número, símbolo u otro dato asignado a una persona que le identifique de manera unívoca a efectos sanitarios; cualquier información acerca de la persona recogida durante la prestación de servicios sanitarios a esta; información derivada de las pruebas o los exámenes de una parte del cuerpo o sustancia corporal, incluidas muestras biológicas; identificación de una persona como prestador de asistencia sanitaria a la persona; o cualquier información sobre, por ejemplo, toda enfermedad, discapacidad, riesgo de enfermedades, historia médica, tratamiento clínico, o estado fisiológico o biomédico real del interesado, independientemente de su fuente, como, por ejemplo, cualquier médico u otro profesional de la sanidad, hospital, dispositivo médico, o prueba diagnóstica in vitro".

El artículo 4 del proyecto de Reglamento recoge las siguientes definiciones: "Datos genéticos: todos los datos, con independencia de su tipo, relativos a las características de una persona que sean hereditarias o adquiridas durante el desarrollo prenatal temprano; Datos relativos a la salud: cualquier información que se refiera a la salud física o mental de una persona, o a la asistencia prestada por los servicios de salud a la persona".

Es obvio que para delimitar el alcance del concepto de dato personal relacionado con la salud, más que a la definición contenida en el artículo 4 habrá que estar a lo establecido en el considerando 26, al constituir éste una herramienta interpretativa del texto articulado. Pues bien, atendiendo a la amplitud dada al concepto, muchos tratamientos de datos que hasta ahora podían considerarse como de nivel de seguridad básico (por ejemplo y entre otros muchos, los ficheros administrativos de tarjeta sanitaria), pasan a tener la consideración de tratamientos de datos especialmente protegidos, lo que implica mayores exigencias, por ejemplo, en materia de obtención del consentimiento del interesado para el tratamiento de sus datos, o la necesidad de implantar mayores medidas de seguridad sobre los mismos.

Como una manifestación específica del "derecho al olvido" que se recoge en el proyecto de Reglamento Europeo, se establece la necesidad, por parte del responsable del tratamiento, de fijar (y cumplir) plazos

determinados para la conservación de los datos, en función de los tratamientos que se realicen. El apartado e) del artículo 5 determina que "los datos personales deberán ser conservados en una forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que se someten a tratamiento; los datos personales podrán ser conservados durante períodos más largos, siempre que se traten exclusivamente para fines de investigación histórica, estadística o científica, con arreglo a las normas y condiciones establecidas en el artículo 83 –con carácter general, conservación separada de los datos identificativos del resto de datos y obtención del consentimiento explícito del interesado– y si se lleva a cabo una revisión periódica para evaluar la necesidad de seguir conservándolos".

Es destacable el deber ineludible de marcar plazos de conservación de los datos personales, de realizar evaluaciones periódicas de la necesidad de seguir conservándolos más allá del plazo establecido para el tratamiento de los mismos –que deberán justificar de forma suficiente esa conservación¬–, así como que se haya incluido entre la información que deberá facilitarse al interesado cuando ejerza el derecho de acceso a la información de su titularidad que está siendo objeto de tratamiento, el plazo establecido para la conservación de dichos datos.

La necesaria revisión de los tratamientos de datos personales que esté realizando el responsable, al objeto de implementar los nuevos requerimientos introducidos por el Proyecto de Reglamento Europeo, deberán realizarse sobre la base de las especificaciones introducidas por el artículo 23 del mismo (Protección de Datos desde el diseño y por defecto): "Habida cuenta de las técnicas existentes y de los costes asociados a su implementación, el responsable del tratamiento implementará, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento sea conforme a las disposiciones del presente Reglamento y garantice la protección de los derechos del interesado". "El responsable del tratamiento implementará mecanismos con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento y, especialmente, que no se recojan y conserven más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación. En concreto, estos mecanismos garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas".

El considerando 70 del Proyecto de Reglamento Europeo prevé le eliminación de la obligación de notificación e inscripción de los tratamientos de datos en los Registro que mantenían las distintas Autoridades de Control. En nuestro caso, con carácter general, en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos –o Registros similares habilitados por las Autoridades de Control Autonómicas–. No obstante, la carga "administrativa" del responsable del tratamiento se ve incrementada por las obligaciones que le asigna el artículo 22 del Proyecto:

"El responsable del tratamiento adoptará políticas e implementará medidas apropiadas para asegurar y poder demostrar que el tratamiento de datos personales se lleva a cabo con el presente Reglamento.

En particular:

a) La conservación de la documentación con arreglo a lo dispuesto en el artículo 28 –Nombre y datos de contacto del responsable del tratamiento, o de cualquier corresponsable o coencargado del tratamiento, y del representante, si lo hubiera; el nombre y los datos de contacto del delegado de protección de datos, si lo hubiera; los fines del tratamiento, en particular los fines legítimos perseguidos por el responsable del tratamiento; una descripción de las categorías de interesados y de las categorías de datos personales que les conciernen; los destinatarios o las categorías de destinatarios de los datos personales, incluidos los responsables del tratamiento a quienes se comuniquen datos personales por el interés legítimo que persiguen; en su caso, las transferencias de datos a un tercer país o a una organización internacional, incluido el nombre de dicho tercer país o de dicha organización internacional y, en el caso de las transferencias contempladas en el artículo 44.1.h), la documentación de las garantías apropiadas; una indicación general de los plazos establecidos para la supresión de las diferentes categorías de datos; la descripción de los mecanismos para verificar la eficacia de las medidas previstas para el cumplimiento de sus obligaciones (siempre que no sea desproporcionado, estas verificaciones serán llevadas a cabo por auditores independientes internos o externos) –.

b) La implementación de los requisitos en materia de seguridad de los datos establecidos en el artículo 30 –A raíz de una evaluación de riesgos, el responsable y el encargado del tratamiento implementarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en relación con los riesgos que entrañe el tratamiento y la naturaleza de los datos personales que deban

protegerse, habida cuenta de las técnicas existentes y de los costes asociados a su implementación–.

c) La realización de una evaluación de impacto en relación con la protección de datos con arreglo a lo dispuesto en el artículo 33 –cuando las operaciones de tratamiento entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines, el responsable o el encargado del tratamiento que actúe por cuenta del responsable llevarán a cabo una evaluación de impacto de las operaciones de tratamiento previstas en la protección de datos personales (aplicable a los tratamientos de daros de salud y genéticos) –.

d) El cumplimiento de los requisitos en materia de autorización o consulta previas de la autoridad de control con arreglo a lo dispuesto en el artículo 34, apartados 1 y 2 –el responsable o el encargado del tratamiento que actúe por cuenta de aquel deberán consultar a la autoridad de control antes de proceder al tratamiento de datos personales a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, sobre todo, de atenuar los riesgos para las interesados cuando: a) una evaluación del impacto en la protección de datos indique que es probable que las operaciones de tratamiento, por su naturaleza, alcance o fines, entrañen un elevado nivel de riesgos específicos; b) la autoridad de control considere necesario proceder a una consulta previa en relación con las operaciones de tratamiento que probablemente entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines–.

e) La designación de un delegado de protección de datos con arreglo a lo dispuesto en el artículo 35.1 –el responsable y el encargado del tratamiento designarán a un delegado de protección de datos siempre que: a) el tratamiento sea llevado a cabo por una autoridad u organismo público, o; b) el tratamiento sea llevado a cabo por una empresa que emplee a doscientas cincuenta personas o más, o; c) las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados–".

today
Atos Origin and Siemens IT Solutions & Services become Atos

Juntos, iniciamos un nuevo viaje que determinará el futuro de las TI

Con presencia en más de 42 países y una plantilla de 78.500 expertos en tecnología aplicada al negocio, ofrecemos a nuestros clientes un profundo conocimiento del mercado, una presencia aún más global y un impresionante portfolio de servicios. Gracias a nuestra trayectoria de 30 años de éxitos y experiencia demostrada en servicios de Consultoría, Servicios Gestionados (número 1 en Europa), Integración de Sistemas, así como servicios de Cloud Computing y actividades basadas en Transacciones, entendemos los retos a los que se enfrenta su negocio y le ofrecemos soluciones de TI que satisfacen sus necesidades, con resultados medibles y sostenibles. ¿Nuestra aspiración? Unir a personas, tecnología y negocio para acelerar el progreso. Hoy, juntos, comenzamos a dar forma al fascinante futuro de las TI y los negocios. Únase a nosotros. **es.atos.net**

Your business technologists. **Powering progress**

Atos

La protección de datos en el día a día de un gerente en un hospital ¿misión imposible?

Rosario Cabezudo Vallés
Directora Hospital Clínico de Zaragoza

El acceso a la historia clínica viene regulado por la Ley 41 de Autonomía del paciente, y por el artículo 15 LOPDP que configura el derecho de acceso como la facultad del individuo de solicitar y obtener gratuitamente información de sus datos personales sometidos a tratamiento, del origen de los mismos y de las comunicaciones realizadas o previstas. Su ejercicio se encuentra sometido a un límite temporal puesto que sólo podrá ejercitarse a intervalos no inferiores a doce meses, salvo que se acredite un interés legítimo que justifique un nuevo acceso.

ACCESO A LA HISTORIA CLÍNICA

Es recomendable no obstante tener en los Centros Sanitarios un documento que recoja las normas de acceso a la historia clínica (HC) y el procedimiento para su acceso, incorporando no sólo el procedimiento del propio paciente para el acceso a su historial, sino el de los familiares una vez fallecido el paciente, en los casos de menores, accesos para docencia, investigación, salud pública, inspección, mutuas patronales, en los casos de derivación a otro Centro Sanitario, etc.

Conviene que exista un documento en el cual cualquiera que solicite el acceso a una historia clínica quede constancia de quien es y la relación con el paciente o cual es el objeto o justificación para su acceso.

El número de Sanitarios que diariamente trabajan en un Centro Sanitario es muy alto y la rotación de personal eventual o de sustitución a lo largo del año, también es muy alto, por ello se les debe de entregar el manual de acceso, incluido un recordatorio del deber de confidencialidad a todos estos profesionales, incluidos los residentes, estudiantes de Medicina, estudiantes de Enfermería, de Psicología, etc.

Tanto el tema del acceso como el de la confidencialidad se debe incluir en las cursos de formación del personal, ya que en el día a día inmersos en el trabajo y constantemente hablando de pacientes, patologías, pruebas, tratamientos, cuando salen del entorno de la planta, de la consulta, del quirófano, siguen hablando entre ellos en otras dependencias no sanitarias como, cafetería, ascensor, pasillos.

El paciente por normativa tiene derecho al acceso a su historia clínica, pero debemos racionalizar las peticiones y evitar las miles de fotocopias que se realizan diariamente en todos los Centros Sanitarios de España, sin sentido y sin utilidad. Aquí iniciaríamos el debate ¿Qué es la Historia Clínica? ¿Qué documentos la componen? ¿Precisan de toda su HC o solo del episodio actual?

En la Ley 41, se recogen los documentos mínimos que deben formar parte de la HC, y en cuanto al acceso a la historia clínica, es importante resaltar que en los casos habilitados legalmente, deberá ajustarse a los principios de calidad y proporcionalidad. Este último supone el deber de limitar el acceso a los datos que efectivamente resulten necesarios para el cumplimiento de la finalidad que justifique dicho acceso, sin que deba extenderse a datos no vinculados a dicha finalidad.

En muchos Centros Sanitarios la mayoría de las solicitudes de fotocopias de HC es por traslado de Ciudad o de Hospital, y debemos darle al paciente lo que verdaderamente le interesa al facultativo que le va a visitar en otro Centro, para garantizar la adecuada asistencia sanitaria.

En segundo lugar le siguen los casos de los pacientes o los familiares que no están de acuerdo con la asistencia recibida. En los casos de familiares de fallecidos hay que ser en extremo cuidadosos y exigir documentalmente la relación con el paciente fallecido y si la relación no es directa, exigir el testamento o documento que acredite que esa tercera persona que lo solicita es verdaderamente quien dice ser. El artículo 18.4 de la Ley 41, expresa que solo se puede facilitar el acceso a la HC a las personas vinculadas al paciente por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. Es muy vago el término "vinculadas", es un criterio tan indefinido como inseguro, pues no aclara si se trata de parentesco en términos legales, por lo que no

sabemos qué grado de consanguinidad admite o si se incluye el de afinidad, de convivientes inscritos en el registro de parejas o de simples personas que han convivido con el fallecido circunstancialmente, pero se antepone el derecho del fallecido a su confidencialidad y a la utilización de su HC para la finalidad asistencial y no para otros fines, procurando siempre conjugar debidamente este derecho con el derecho a la intimidad del paciente y el deber de secreto.

Relacionado con el acceso, hay un tema que no esta en absoluto resuelto y es la solicitud de un paciente a la prohibición de acceso a sus datos o a su HC, a dar información sobre consultas, ingresos y otros contactos con el Centro Sanitario, es un derecho del paciente y es difícil llevarlo a la práctica en la HC informatizada y en la información general del hospital o en las propias plantas o consultas, en relación con esto, esta sin resolver si una vez fallecido se extingue este derecho y si los familiares alegando un riesgo para su salud tienen derecho a una HC sobre la cual el paciente expreso su derecho de prohibición de acceso.

En cuanto a los accesos a la HC para investigación, docencia, están claros los fines por los que se puede acceder y el investigador, docente, debe comprometerse por escrito a solo utilizar los datos para investigación y a cumplir con la normativa de protección de datos. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínicoasistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlo

Las notas, aportaciones subjetivas en principio no se deben incluir en las fotocopias de la HC, si lo solicitan explícitamente hay que preguntar al Facultativo o Enfermera si quieren que se les de o quieren quitarlo, aunque no queda claro en la normativa. Estas anotaciones o apreciaciones subjetivas se deben generar en interés del paciente.

El Código de Deontología Médica en el articulo 19 dice que "El médico tiene el deber y el derecho de redactar la HC incorporando la información que se considere relevante para el conocimiento de la salud del paciente".

Desprestigiar las anotaciones subjetivas nos podrá llevar a elaborar historias clínicas empobrecidas, intelectualmente y literalmente, llevadas por una intensiva tendencia a evitar complicaciones ante un eventual acceso de los pacientes, esto podría suponer la muerte lenta de la HC.

ACCESO A LA HISTORIA CLÍNICA INFORMATIZADA

Cada profesional debe tener una clave de acceso personal e intransferible y el único responsable de cesión, copia de la clave de acceso es el profesional. El sistema que este implantado en el Centro Sanitario, identificará de forma inequívoca y personalizada a todo profesional que intente acceder a la historia clínica electrónica, se tendrá registros de accesos y de trazabilidad.

Hay que erradicar la cultura o costumbre de los profesionales sanitarios que por comodidad o por no desconocimiento del manejo de la HC informatizada, dan la clave a otro profesional, Enfermería, Auxiliar, Residente, para que realicen el informe, extraigan los resultados de pruebas, etc. Adjunto un artículo en un bloog llamado "Heraldo Sanitario de Oregón" en el cual se critica la prohibición que se dicto de que las Auxiliares de Enfermería impriman los resultados analíticos, quienes escriben son Facultativos:

"Los médicos del hospital ¿?? de todas las categorías desde adjuntos hasta jefes de servicio han sido obligados recientemente a realizar labores de auxiliares de clínica en las consultas externas. Se trata de las labores previas a la consulta como la extracción, impresión de resultados de análisis clínicos, pruebas radiológicas, ecografías, gammagrafías, etc., labores que hasta hace poco eran desempeñadas por las auxiliares de clínica. La Dirección ha prohibido a las auxiliares de clínica entrar en la base de datos con el fin de buscar e imprimir analíticas, informes de pruebas complementarios con el fin de que los facultativos no tuvieran que perder el tiempo en labores burocráticas que no le son propias. La dirección ha prohibido terminantemente a las auxiliares utilizar las claves de los facultativos para acceder a los datos informáticas de los pacientes." (Publicado en el año 2012)

Creo que es suficientemente representativo de la poca conciencia que tienen los Facultativos de que su clave es personal y que solo ellos pueden acceder a los datos clínicos con su clave y no terceras personas.

Resulta necesario que la normativa preste especial atención al auge de la historia clínica electrónica, con los peligros que ello conlleva en relación con los posibles accesos no autorizados a la misma en la actual sociedad de la información. En este sentido se propone la revisión de la legislación a fin de articular un mecanismo uniforme para el control del acceso al historial clínico al mismo tiempo que

se refuerzan las garantías para la intimidad de los pacientes y para la protección de sus datos con el objetivo de evitar la disparidad de criterios

CANCELACIÓN O MODIFICACIÓN DE DATOS

Si los datos son de salud, antecedentes médicos personales, antecedentes familiares y que pueden ser importantes para el desarrollo o diagnostico de enfermedades, son pertinentes y no excesivos para la finalidad de la HC, que no es otra que la asistencia al paciente mediante el conocimiento de todas las patologías

El principio de calidad de datos (que los datos sean veraces y estén actualizados) tiene gran trascendencia en los datos recogidos en la historia clínica. La normativa no ha regulado este derecho, ya que, dada la particularidad de la materia, deberían haberse matizado cuestiones tales como que documentación es necesaria para rectificar o cancelar la historia clínica, plazos de verificación del error del dato, la puede realizar cualquier profesional o el que incluyó el dato erróneo, etc... Y además ¿Quién podría cancelarlas? ¿El propio médico? ¿Un compañero? ¿La Comisión de historias clínicas del Centro?

Diariamente nos encontramos con casos concretos que se deben resolver de maneras diferentes en dependencia del caso y siempre cumpliendo la normativa y preservando la integridad de la HC, así, si una paciente acude a Urgencias por una fractura de codo y en el informe consta que de joven consumió drogas, ella pide la modificación de este dato en el informe de urgencias, porque la empresa le pide un informe justificativo de su baja laboral, se valora y se decide que es importante este dato en la HC, pero no en el informe de urgencias. Se le realiza un informe clínico del episodio de la fractura de codo, sin mencionar antecedentes personales y se mantiene el dato en la historia, la usuaria queda conforme. Son casos individuales y hay que buscar soluciones individuales, ya que la normativa no las tiene previstas.

La revolución del reconocimiento
de voz para la movilidad en sanidad:
EN LA NUBE.
DONDE QUIERA.
CUANDO QUIERA.
La nueva 360 | Development Platform.
La única oferta de servicios de reconocimiento de voz
de cloud y movilidad para la documentación clínica.
360
www.nuance.es | sanidad@nuance.com
NUANCE

SUMMA 112

SaludMadrid

Comunidad de Madrid

Dispositivos móviles (MCA) en la atención a urgencias y emergencias médicas



"La ambulancia sin papeles"

Retos

La atención a urgencias y emergencias médicas es un claro ejemplo de proceso en el que la agilidad y la seguridad en las actuaciones y en la toma de decisiones es de vital trascendencia. Para ello, los profesionales implicados, además de contar con la experiencia, conocimiento y especialización adecuados, precisan disponer de toda la información necesaria, exactamente en el momento y en el lugar adecuados.

La utilización de dispositivos móviles (MCA – Mobile Clinical Assistant) en éste escenario de atención, debe permitir a los profesionales sanitarios acceder a sus sistemas de información y disponer de la información clínica y de las herramientas de ayuda a la toma de decisiones en el punto de asistencia, sustituyendo, además, la utilización del soporte papel, completando el "circuito asistencial digital".

Éste reto ha sido asumido en el Servicio de Urgencias Médicas de Madrid (SUMMA 112). Con la finalidad de evaluar la utilidad de los dispositivos móviles MCA en su trabajo diario, se ha realizado un análisis del proceso asistencial antes y después de su utilización, que ha permitido observar mejoras en la eficiencia así como del la calidad y gestión de la información asociada.

EL SUMMA112

El SUMMA 112 es responsable de la atención a las urgencias y emergencias extrahospitalarias en la Comunidad de Madrid. Para ilustrar la demanda y creación de información derivada de su actividad, se recogen a continuación algunas cifras de actividad (por año):

- Número de llamadas atendidas: 1.009.474
- Número de actuaciones de las UVI Móviles: 77.725
- Número de actuaciones de los Vehículos de Intervención Rápida: 33.624
- Número de actuaciones de la Unidad de Atención Domiciliaria: 108.135

Ésta actividad supone la generación y utilización de una enorme cantidad de información, que ha de fluir rápidamente y de manera segura y fiable: es por eso, que la utilización de Sistemas de Información adecuados y de las herramientas necesarias, adaptadas a éste entorno, y de solvencia contrastada, es fundamental. La dotación de dispositivos MCA por parte del SUMMA 112, está permitiendo a sus profesionales disponer de la información adecuada, independientemente de donde tengan que llevar a cabo la atención sanitaria, de una manera rápida y fiable.

Soluciones: El apoyo del MCA en el proceso asistencial del SUMMA112

Los vehículos asistenciales del SUMMA 112 están dotados de un MCA con conexión GPRs, comunicado con el Servicio Coordinador de Urgencias (SCU), e integrado con el sistema de información del Summa 112, lo que hace posible el intercambio de toda la información relativa a la gestión de la propia intervención, (llegada al lugar de la intervención, traslado al paciente al hospital, finalización de la intervención, etc.), así como los datos clínicos del paciente.

En el momento en que el SCU asigna una intervención a un recurso asistencial, automáticamente llega al MCA de la unidad asistencial, la información acerca del caso, de la intervención y los datos más relevantes del paciente: dirección del punto de asistencia, resultado del algoritmo de clasificación, edad, síntomas capturados por el facultativo, edad, etc. El equipo asistencial, mediante el MCA, informa al SCU, en tiempo real, del estado de situación de la intervención en cada momento, mediante mensajes que aparecen en la aplicación de gestión de recursos de la central; en caso de que el que el dispositivo se encuentre sin cobertura, continúa trabajando sin conexión a red,

Atos

intel Health

enviándose las actualizaciones en el momento en el que esta última se restableciese.

La función principal del MCA es la cumplimentación del Informe Asistencial mediante una aplicación desarrollada para tal fin. Dispone de una secuencia de pantallas (con punteo táctil), que abarcan la valoración inicial y los signos y síntomas por sistemas y aparatos del cuerpo humano; las pruebas complementarias que se realizan al paciente durante la actuación del equipo médico, (electrocardiografía, tensión arterial, pulsioximetría, medición de monóxido de carbono, etc.), son enviados desde el aparataje electromédico, vía bluetooth, al MCA, integrándose los datos en el propio informe asistencial.

Desde el Sistema de Información del SCU y desde el propio MCA, se tiene acceso al Visor de Historia Clínica Electrónica de la Consejería de Sanidad de Madrid, de forma que el profesional sanitario puede consultar aspectos relevantes relativos a la situación de salud del paciente distribuidos en los sistemas de información asistencial (antecedentes de salud, diagnósticos previos, tratamientos, etc.), que pueden permitir actuar de forma más rápida al paciente, y dar una asistencia de mayor calidad, teniendo en cuenta toda esa información disponible en los diferentes Centros Sanitarios.

Una vez realizada la asistencia, y cumplimentado el informe asistencial, la integración con el Visor de Historia Clínica Electrónica hace posible que la información esté accesible desde dicho Visor, de forma que el Hospital de destino se tiene disponible el "Informe Asistencial", haciendo innecesaria la entrega de informe en papel, en caso de ingreso. Así mismo, desde los Equipos de Atención Primaria, tendrán la información disponible de todas las actuaciones de emergencias y urgencias relaccionadas con sus pacientes, facilitando de este modo el seguimiento y evolución de los mismos. Además, el sistema tiene la opción de impresión del informe asistencial para entregar al paciente en el momento de la actuación.

Beneficios y Mejoras: el valor aportado por el MCA en los servicios del SUMMA112

El análisis realizado durante la fase inicial de la implantación en las unidades móviles del SUMMA112, llevado a cabo mediante observación del proceso asistencial y la realización de algunas mediciones de tiempo y encuesta a los profesionales sanitarios, ha permitido observar nuevas mejoras en un servicio que, ya de origen, dispone de altos niveles de calidad y eficiencia.

La incorporación del MCA a los equipos de intervención, y por tanto, del acceso a los sistemas de información en movilidad, ha abierto la posibilidad de sistematizar tareas y mejorar procesos, tanto asistenciales como de soporte, aportando sencillez e inmediatez a la gestión del proceso.

Algunos ejemplos del valor añadido por el uso del MCA son:

Integración con otros niveles asistenciales y Continuidad asistencial: la utilización del visor de Historia Clínica Electrónica de la Comunidad de Madrid, en movilidad, permite que la información de las actuaciones del SUMMA 112, estén disponibles para el resto de niveles asistenciales, en tiempo real, y a la inversa, el acceso a los datos del paciente que están distribuidos en los diferentes Sistemas de Información asistenciales de la Comunidad de Madrid, hacen posible la cooperación con los distintos niveles asistenciales, la utilización conjunta de la información clínica, y, en definitiva la continuidad asistencial.

Gestión de la atención en la Urgencia hospitalaria: la comunicación de pre-ingreso de pacientes y el envío del informe asistencial en tiempo real, permiten optimizar la gestión de la atención en el Hospital, con una mejor preparación y disponibilidad de recursos a la llegada del paciente.

Comunicación entre los profesionales del SUMMA y con el resto del sistema: a posibilidad de acceso al correo electrónico y a la intranet sanitaria, desde el MCA, permite una mejor comunicación, en movilidad, del personal embarcado.

Eliminación de posibles errores en la transmisión de información: al automatizar el proceso de recogida de información, envío y posterior introducción en el sistema, se eliminan los posibles errores que pueden aparecer en todo proceso manual.

Acceso, en movilidad, a recursos de conocimiento y herramientas de apoyo a la decisión: con el acceso a la intranet del Servicio y de la propia Consejería de Sanidad, se hace posible, en movilidad, y de forma inmedita, la difusión protocolos, información de carácter formativo, acceso a Vademécum, bibliografía, etc.

Mejoras en la logística asistencial: diversas aplicaciones dan cobertura, en tiempo real, a los procedimientos relacionados con la logística asistencial (Hoja de relevo de la guardia, revisión de carros de parada, oxígeno, etc.). Asimismo, hace posible la solicitud automática de recursos en situaciones prefijadas.

Mejoras en la gestión de recursos humanos: la información de los registros de personal se obtiene en tiempo real permitiendo optimizar eficiencias.

Notificación de incidencias y peticiones de material: el personal de las unidades asistenciales, en tiempo real, realiza la notificación de incidencias y peticiones de material que, de otra forma, tendrían que hacerse tras concluir los servicios.

Algunos de los beneficios objetivables mediante mediciones de tiempos de procesos se expresan en la tabla:

Indicador analizado	Antes de MCA	Con MCA
Tiempo dedicado a transmitir la información relevante de la asistencia por parte de la SCU al personal de la unidad móvil	3 min	Online
Tiempo para la asignación de los recursos a un determinado incidente con necesidad de atención	5 min	Online
Tiempo dedicado a la información sobre el estado de la intervención a la central	3 min	Online
Consulta de la información asistencial del paciente en los centros de la Consejería de Sanidad de Madrid	No viable	Posible (1 min)

Referencias

www.intel.cm/healthcare/ps/mca
http://www.intel.com/it/pdf/measuring-it-success-at-the-bottom-line.pdf
http://www.intel.com/intelpress/sum_bvm.htm
http://www.intel.com/healthcare/hit/providers/hit_value_model_whitepaper.pdf

SUMMA 112 SaludMadrid Comunidad de Madrid

Atos

intel

Una introducción al impacto del "cloud computing"

Ramón Miralles
Coordinador de Auditoria y Seguridad de la Información
Autoridad Catalana de Protección de Datos

Se ha escrito ya mucho sobre el "cloud computing", y des de muchas perspectivas, y sin duda aún queda mucho por escribir, y sobretodo por explicar; aquí sin ánimo de ir más allá de una introducción y sin llegar a la profundidad que requerirían algunas de las cuestiones que abordaré, planteo este artículo como una primera y ligera aproximación a los servicios en "cloud", y como no podría ser de otro modo, haré algunos breves apuntes sobre el impacto general que sobre el tratamiento de datos de carácter personal puede tener el "cloud computing".

El "cloud computing" es una arquitectura o modelo de prestación i/o aprovisionamiento de servicios de tecnologías de la información y la comunicación que cada vez está asumiendo más protagonismo. Según los más expertos analistas, en los próximos años se consolidará tanto por lo que respecta al usuario doméstico, como a las empresas y administraciones públicas, en un futuro no muy lejano toda o casi toda la información se procesará en la nube.

Mi primer contacto profesional con el concepto de "cloud computing" fue a través de un documento de mayo de 2008, concretamente un "white paper" de la oficina del Comisionado de Información y Privacidad de Ontario (Canadá): "Privacy in the clouds".

El documento en si mismo no aporta, en estos momentos, una reflexión relevante en cuanto a la protección de datos personales y el "cloud computing", ya que se dedica fundamentalmente a la identidad digital en Internet.

Hay otro documento, también del IPC de Ontario, que sí que aborda con más profundidad la cuestión de la privacidad y el "cloud computing": "Modeling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach" publicado en mayo de 2010.

En cuanto al origen del concepto de "cloud computing". Desde la óptica de las telecomunicaciones se entiende por "cloud" o "nube", el conjunto de dispositivos e infraestructuras de comunicaciones por los cuales, de manera "impredecible", pasa la información cuando se transmite de un punto a otro de la red (Internet); esa relativa falta de predicción afecta tanto al número como al tipo de dispositivos.

De hecho tradicionalmente todos los elementos que se encuentran involucrados en esos intercambios de información se han representado gráficamente ubicados en una "nube".

El punto de inicio de la comunicación es conocido (un usuario o proceso inicia una transacción), y el de destino también (un servidor responde a la transacción), y así sucesivamente. Pero el camino que seguirá la información transportada entre esos dos puntos responde a unas reglas que, si bien están fijadas por un protocolo técnico (TCP), tienen resultados en general impredecibles a priori; de manera que en la práctica solo podemos intuir por donde pasará la información.

Hay que añadir otra variable, ya que todo y que en esencia esos dispositivos de red se dedican a gestionar el transito de la información entre origen y destino, no se nos puede escapar que durante ese tránsito la información puede ser sometida a tratamientos que vayan más allá de facilitar la transmisión de paquetes de información.

Aquí abro un paréntesis, solo recordar de manera breve, las tecnologías de inspección de paquetes ("Deep Packet Inspection", DPI), es decir, la capacidad que tienen algunos equipos de red, que no son punto final de la comunicación, de tractar no solo los encabezados de los paquetes que deben transmitir y transportar por la red, si no también, cuando están convenientemente configurados, de analizar su contenido.

Pues bien, cerrando el paréntesis, en el momento en el que la "nube" deja de ser exclusivamente un medio de transporte de la información, para pasar a tener capacidad de procesamiento de la información, se le añade el "computing"; todo y que en realidad la capacidad de procesamiento no recae exactamente en la "nube", si no en aplicaciones, plataformas e infraestructuras disponibles en la red, y que, en al-

gunos aspectos, se comportan como los dispositivos de la "nube" a que he hecho referencia.

El "cloud computing" implica que en el procesamiento de la información concurren una serie de características que tienen como consecuencia directa que el origen, y especialmente el destino de una transacción, dejan de tener unos valores absolutos, para pasar a ser relativos: la información no siempre está ni se trata donde podría parecer.

La definición de "cloud computing" que generalmente sirve de base para dotar de contenido al concepto es la del NIST (Instituto Nacional de Estándares y Tecnologías, una agencia del "US Department of Commerce", creada el año 1901). La última versión de la definición de "cloud computing" elaborada por el NIST es de septiembre de 2011, la encontraremos en el documento "The NIST Definition of Cloud Computing" (SP 800-145).

El NIST considera 5 características como esenciales en el modelo "cloud":

- Autoservicio: el usuario puede utilizar más capacidad de procesamiento o de almacenamiento de la información, sin solicitarlo expresa o directamente al proveedor del servicio.
- Amplio acceso: se puede acceder al servicio desde cualquier conexión a la red y desde cualquier tipo de dispositivo.
- Agrupación y reserva de recursos: hay un conjunto de recursos compartidos por los usuarios, de acuerdo con sus necesidades puntuales, ello implica que en cada momento los recursos reservados pueden ser diferentes.
- Rapidez y elasticidad: se puede acceder a nuevos recursos o capacidades de forma inmediata y aparentemente ilimitada.
- Servicio medible y con supervisión: se controla el uso en todo momento, y se puede conocer, de manera transparente y directa, el nivel de recursos utilizados o consumidos en cada momento.

Esta capacidad de procesamiento en la "nube" está conectada con la ya tradicional y consolidada tendencia a la externalización de los servicios TIC y la reconversión de estos en lo que se ha venido en llamar una "utility computing".

En relación a esta cuestión recomiendo la lectura del artículo de Nicholas Carr, publicado en el "MIT Sloan Management Review" (Massachusetts Institute of Technology), de abril de 2005, que con el título "The End of Corporate Computing" identifica y describe los motivos que han de llevar a las organizaciones a dejar de considerar las TIC como un activo de su propiedad, para pasar a ser un servicio que compran y por el cual pagan exclusivamente por su uso.

En su artículo Carr hace un paralelismo entre el proceso de transformación del uso de las TIC que han de seguir las organizaciones para ser competitivas, con la transformación que se produjo a principios del siglo XX, cuando las empresas industriales empezaron a cerrar y a desmantelar las fuentes de energía utilizadas por sus industrias y que eran de su propiedad (ruedas en saltos de agua, máquinas a vapor, generadores eléctricos, etc.).

Aproximadamente a partir de 1880 la producción comercial de electricidad empezó a ser posible; en 1902, en los Estados Unidos había unas 50.000 plantas de generación privada de energía y solo 3.600 de esas estaciones podían vender excedentes de energía a otras industrias, eso si, al principio con muchas limitaciones y a un precio alto. Pero entre 1907 y 1920 la cuota de producción de energía eléctrica que se comercializaba pasó del 40% al 70%, y en 1930 ya llegaba al 80%.

Los motivos para la rápida adopción de un nuevo modelo de subministro de energía para las industrias fueron: unos costos menores y una complejidad de gestión menor, que permitía que las industries pudieran centrarse en su negocio.

En opinión de Nicholas Carr, en su artículo del 2005, hay 3 avances tecnológicos clave en la transformación de las TI: la virtualización, el "grid computing" y los servicios "web" que, combinados con el aumento de capacidad de les redes de comunicaciones y el despliegue de la fibra óptica, generan un escenario idóneo para esa transformación, donde la mayor dificultad para el cambio no será la tecnología, sino la actitud de las organizaciones a la hora de asumir este nuevo modelo de consumo de las TIC en sus negocios.

Lo cierto es que el "cloud computing" ya es una realidad para los usuarios de la red, al menos a título individual. Los principales casos de uso del "cloud computing" implican a compañías y servicios como Facebook, Amazon, Google o Microsoft.

La explosión definitiva del "cloud computing" vendrá provocada por el uso que hagan las empresas, en todo caso tal y como han expresado investigadores del NIST el "cloud computing" es un paradigma que aún está en evolución.

Si hacemos una primera aproximación al impacto sobre la protección de datos de carácter personal, veremos que muchos de los servicios en línea que han emergido como consecuencia del uso social, intensivo y masivo la red, en los últimos años, han puesto al límite a la legislación europea en la materia; de hecho hay que reconocer que en algún caso incluso la legislación ha resultado insuficiente para dar una respuesta óptima a esas nuevas situaciones.

El grupo de autoridades de control que crea el artículo 29 de la Directiva de protección de datos (conocido como el grup del artículo 29) tiene entre sus funciones analizar y dictaminar sobre aquellas cuestiones puedan incidir en las de la Directiva, en su programa de trabajo para el período 2010-2011 se incluía explícitamente analizar el "cloud computing" en relación a la protección de datos de carácter personal.

La Sra. Neelie Kros, Vice-presidenta de la Comisión Europea para la Agenda Digital Europea, en una conferencia pronunciada a finales del 2010 en la Universidad Paris-Dauphine, ya afirmaba que: "A cloud without robust data protection is not the sort of cloud we need".

Que se trata de una cuestión que requiere atención lo ponen en evidencia las consultas públicas que en relación al "cloud computing" han planteado tanto la Comisión Europea, la CNIL o la Agencia Española de Protección de Datos, y especialmente el anuncio, por parte de la Sra. Kros, a principios de este 2012, de la creación de la "European Cloud Partnership"', cuyo objetivo será buscar términos comunes de contratación de servicios "cloud" y desarrollar estándares que garanticen la seguridad y la competencia, con el fin de generar confianza en el mercado de la computación en la nube.

Uno de los documentos que ha servido de base para la reforma de la protección de datos en Europa, y que ahora se está discutiendo en forma de borrador de «Reglamento Europeo de protección de datos», fue una comunicación de la Comisión al Parlamento Europeo y al resto de las principales instituciones de la Unión Europea, de 4 de noviembre de 2010, que bajo el título de "Un enfoque global de la protección de los datos personales en la Unión Europea" identificaba los objetivos esenciales de esa reforma.

Pues bien, en su introducción, se destacaba que si bien los principios de la Directiva de protección de datos del año 95 seguían siendo válidos, la "rapidez de la evolución tecnológica y la globalización" planteaban nuevos retos en materia de protección de los datos personales.

Entre otros fenómenos de uso intensivo por parte de los ciudadanos de las tecnologías de la información y la comunicación, se hace referencia en ese documento a que la computación en nube plantea retos para la protección de datos, "dado que puede implicar la pérdida del control por parte de los individuos de su información potencialmente sensible cuando almacenan sus datos utilizando" servicios alojados en la nube.

Y es que los diferentes modelos de servicios de "cloud computing", ya sea de aplicaciones (SaaS), de plataforma (PaaS) o de infraestructura (IaaS), impactan directamente sobre una cuestión clave en la definición del derecho a la protección de datos de carácter: la autodeterminación informativa. En función del modelo de despliegue del servicio "cloud" el impacto obviamente será de mayor o menor intensidad: nube pública, privada o híbrida. Como ya avanzaba uno de los principales inconvenientes detectados en relación al "cloud computing" es la pérdida efectiva de control sobre los datos, ya que más allá de los vínculos contractuales o de subscripción a los servicios, desaparece o al menos se diluye la certeza sobre la ubicación física de la información y sobre las condiciones de procesamiento y, en consecuencia, pueden quedar afectadas las garantías de confidencialidad y de seguridad, de la información situada en la nube.

No se trata de una preocupación expresada únicamente por las autoridades de control, ya que tal y como recoge un documento del NIST, de julio de 2009, "Effectively and Securely Using the Cloud Computing Paradigm", uno de los retos del cloud computing es la seguridad, todo y que el propio documento valora que la "cloud security is a tractable problem".

Tan solo se trataba de hacer una introducción al tema, pero no quisiera dejar pasar la oportunidad de concluir identificando los aspectos más relevantes relacionados con los marcos normativos de protección de datos de carácter personal:

1. La pérdida de control sobre el tratamiento de la información, tanto por parte de las personas afectadas como por parte del responsable del tratamiento, y las consecuencias que se puedan derivar (seguridad, confidencialidad, ejercicio de derechos, etc.).
2. Las dificultades de encajar jurídicamente, y con suficiente agilidad, las situaciones de tratamiento de los datos por cuenta de terceros: encargados del tratamiento en cloud y las cadenas de subcontrataciones.
3. Las cuestiones relacionadas con el movimiento internacional de datos.
4. Y por último, la resolución efectiva de los incidentes relacionados con la vulneración del derecho fundamental a la protección de datos personales en situaciones de multiterritorialidad.

En relación a los aspectos de cumplimiento legal resulta de utilidad la consulta del "Cloud Compliance Report", de mayo de 2011, elaborado por un numeroso grupo de expertos coordinados por el capítulo español de la "Cloud Security Alliance", que incluye todo un capítulo dedicado al "Cumplimiento legislativo en materia de privacidad".

Seguridad, protección de datos y responsabilidad en Cloud Computing

Nathaly Rey
Directora de ISMS Forum Spain
Miembro del Board de Cloud Security Alliance, España

La seguridad de la información constituye una de las principales barreras para la adopción de soluciones de Cloud Computing dentro de las organizaciones. No obstante, la nube también constituye una forma, a veces la única, de dotar de seguridad a la información corporativa. Por un lado, subir a la nube podría implicar que un tercero llegue a procesar en su infraestructura y de forma deslocalizada, información muy valiosa para la organización y sobre la que recaen numerosas obligaciones cuyo cumplimiento atañe al usuario. Por otro lado, los proveedores de Cloud Computing tienen la capacidad de generar economías de escala muy significativas, que permiten desplegar recursos, competencias y capacidades en materia de seguridad, inalcanzables para la mayoría de las organizaciones.

Los ciberataques y los incidentes relacionados la seguridad han experimentado un crecimiento frenético. La motivación de los atacantes ha pasado de ser la notoriedad y el reconocimiento público, a la obtención de grandes sumas de dinero a través del apoderamiento de registros, de propiedad intelectual y de la I + D de las organizaciones[1]. Ante este panorama, las infraestructuras que se concentran datos de cientos o miles de clientes, como es el caso de las que soportan servicios de Cloud, resultan un objetivo atractivo para los atacantes. Si los atacantes quieren datos, irán a buscarlos allí donde estén. En este sentido, las preocupaciones relacionadas con la responsabilidad del proveedor de Cloud ante incidentes de seguridad, y en particular, frente a daños ocasionados por posibles sanciones pecuniarias ante vulneración de normas, indemnización a titulares de datos personales, y frente a otros más difíciles de cuantificar, como los afectan a la propiedad intelectual, reputación e imagen de las compañías, es una preocupación creciente.

La externalización no es un fenómeno nuevo, sin embargo, factores como la **gran concentración de datos,** la **deslocalización** de su tratamiento, y el **incremento de la conectividad** que se producen con la adopción de modelos de externalización en Cloud, junto a la evolución de las **ciberamenazas,** hacen que los riesgos de seguridad deban gestionarse de forma distinta frente al outsourcing tradicional, cuestión en la que se trabaja intensamente desde grupos como Cloud Security Alliance, y entre otras cosas, que sea imprescindible **delimitar contractualmente** los **criterios para determinar la responsabilidad del proveedor** que custodia los datos, ante incidentes que vulneren su seguridad.

En caso de contratos sometidos a legislación de sistema anglosajón, son habituales las limitaciones de responsabilidad de los prestadores de servicio y, en particular, la determinación de una cantidad económica máxima. No obstante, dichas previsiones son contrarias a las legislaciones del sistema continental, como la nuestra, en la que la responsabilidad será determinada por parámetros como la culpa o negligencia del proveedor, en el marco del incidente.

Si en una prestación de servicios de Cloud resultara de aplicación el derecho sustantivo español en materia de protección de datos personales, independientemente del acuerdo que exista entre las partes sobre la por incumplimiento de las normas, el afectado siempre tendrá derecho a ser indemnizado ante cualquier perjuicio que se le cause.

La acción indemnizatoria por la vulneración del derecho fundamental a la protección de datos de carácter personal, se encuentra consagrada el art. 19.1 de la LOPD, en los términos siguientes: *"Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o encargado del tratamiento, sufran daño*

[1] *El hacktivismo se incorporó como una nueva motivación en 2011con el surgimiento de grupos como Anonymus y que LulzSec.*

o lesión en sus bienes o derechos tendrán derecho a ser indemnizados".

Con esta disposición, el ordenamiento jurídico español da respuesta a la exigencia comunitaria establecida el art. 23 de la Directiva 95/46/CE[2], a tenor del cual, los Estados miembros deben garantizar que *"Toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido, sin perjuicio de que pueda ser eximido, total o parcialmente, de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño".*

Cualquier afectado por los fallos de seguridad de los servicios de Cloud Computing tiene la posibilidad de acudir a los órganos judiciales, el cese de la actividad lesiva y, en su caso, la indemnización de daños y perjuicios ocasionados por la vulneración que ha sufrido como consecuencia del incumplimiento de la norma por parte de quien estaba obligado a ello (arts. 13 y 19 de la LOPD), sin perjuicio de la posibilidad de activar el aparato administrativo del Estado[3], para que se proceda a la imposición de sanciones a los responsables de los ficheros de datos personales y de los encargados de su tratamiento, según corresponda.

Tanto de la LOPD, como de la Directiva, se desprende que no se trata de un sistema de responsabilidad objetiva, sino de un sistema de responsabilidad basado en la culpa o negligencia mediante el incumplimiento de la normativa de protección de datos, que devenga en un perjuicio para el afectado. Por tanto, si no ha habido inobservancia de las normas de protección de datos , aunque haya habido lesión por un incidente en la seguridad de los datos[4], no habrá lugar a esta acción indemnizatoria.

Fuera del ámbito de la normativa sobre protección de datos personales, determinar la existencia de negligencia es una cuestión compleja. No existe jurisprudencia que sirva como referente en la industria para configurarla en el marco de un incidente de seguridad. Ahora bien, el concepto viene ligado a lo que se considera **objetivamente razonable.** En este sentido, parece razonable que lo que se exija sea la perfecta aplicación de lo pactado en el contrato y el Acuerdo de Nivel de Servicio (SLA) y en su caso en el Privacy Level Agreement (PLA), y que constituyan estos el el marco de actuación que eventualmente pueda utilizarse para determinar la culpa o negligencia del proveedor. Evidentemente, el usuario deberá poder valorar ex ante si este marco le parece **objetivamente razonable.** Esta aproximación implica que se compartan los riesgos y las responsabilidades en el tratamiento de los datos. Otra aproximación implicaría que el proveedor asumiera una responsabilidad ilimitada, si esto ocurriera en el marco de la relación a sus cientos o miles de cliente, probablemente su beneficio tendería a desaparecer.

Los costes de un incidente de seguridad pueden ser altos, según un estudio de *Ponemon Institute,* el coste por cada registro de cliente oscila entre 58 y 200 euros, dependiendo del sector afectado. Por su parte, Sony atribuyó unos costes de 132 millones de euros a los ataques a su red de PlayStation en 2011, los cuales pusieron en peligro los datos personales de alrededor 100 millones de clientes. De allí que los seguros sobre ciber riesgos sean un elemento traído a colación, cada vez más, en la negociación entre las partes.

---

[2] Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[3] El ordenamiento jurídico español, ha establecido autoridades garantes de naturaleza administrativa como la AEPD y las agencias autonómicas de protección de datos, a las que se atribuyen funciones preventivas y sancionadoras (arts. 18, 44 y 45 de la LOPD), cuyo objeto de declarar si hay lugar a una infracción administrativa, y en su caso, sancionar a autor de dicha infracción a la luz del artículo 43.1 que establece que "los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley".

[4] Contenidas fundamentalmente en la Ley Orgánica15/1999 de protección de datos de carácter personal, y su reglamento de desarrollo, el Real Decreto 1720/2007.

Dudas y soluciones en relación con algunas cuestiones recurrentes en protección de datos de salud

Emilio del Val Puerto
Subdirector General de Inspección y Tutela de Derechos
Agencia de Protección de Datos de la Comunidad de Madrid

Del carácter multidisciplinar predicable de la protección de datos de carácter personal, derivan –en materia de salud- múltiples cuestiones merecedoras de un análisis pormenorizado. Sin embargo, en este breve artículo, mi intención pasa –únicamente- por la exposición de la complejidad inherente a algunas de ellas, y el análisis de las soluciones que, por parte de la Agencia de Protección de Datos de la Comunidad de Madrid, se han adoptado en relación con las mismas.

NATURALEZA DE LOS DATOS CONTENIDOS EN LOS INFORMES E HISTORIALES DE PERSONAS FALLECIDAS

La resolución de la cuestión planteada debe obtenerse en función de la naturaleza misma del derecho protegido por la norma, lo que conduce a la necesidad de determinar si la muerte de las personas da lugar a la extinción del derecho a la protección de la "privacidad" o al derecho a la "protección de los datos de carácter personal", regulado por la LOPD, ya que el artículo 32 del Código Civil dispone que "la personalidad civil se extingue por la muerte de las personas", lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.

De acuerdo con la doctrina consolidada por la AEPD y por el resto de Autoridades de Control españolas, si el derecho fundamental a la protección de datos ha de ser concebido como un derecho de la personalidad que otorga al individuo un poder de disposición sobre la información que le concierne, en los términos expuestos por el Tribunal Constitucional 292/2000, de 30 de noviembre, el fallecimiento del individuo, produciría, por aplicación del artículo 32 del Código Civil, la extinción de dicho derecho, sin perjuicio de la subsistencia de las acciones que procedan para preservar el honor de la persona fallecida, conforme a lo dispuesto en la citada Ley Orgánica 1/1982, de 5 de mayo.

En razón de lo señalado, si un supuesto de hecho concreto se refiere exclusivamente a personas fallecidas, no se encontraría, en principio, sometido al régimen previsto en la LOPD, y, en consecuencia, desde la perspectiva de la normativa sobre protección de datos, no cabría hablar de ficheros con datos de carácter personal.

En este sentido, el artículo 2.4 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, referido a su "Ámbito objetivo de aplicación", establece que este Reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

No obstante, si bien el derecho a la protección de datos pudiera desaparecer como consecuencia de la muerte de las personas, no sucede así con el derecho de determinadas personas para ejercitar acciones en nombre de las personas fallecidas, con el fin de garantizar otros derechos constitucionalmente reconocidos. Así, por ejemplo, cabe destacar que la Ley Orgánica 1/1982, de 5 de mayo, pone de manifiesto, en sus artículos 4 a 6, que el fallecimiento no impide que por las personas que enumera el primero de los preceptos citados puedan ejercitarse las acciones correspondientes, siendo éstas la persona que el difunto haya desig-

nado a tal efecto en testamento, su cónyuge, ascendientes, descendientes o hermanos que viviesen al tiempo de su fallecimiento o, a falta de las personas anteriormente citadas, el Ministerio Fiscal.

En relación con los "Derechos de acceso a la historia clínica", también conviene recordar que la Ley 41/2002, de 14 de noviembre, básica reguladora de "la autonomía del paciente", reconoce, en su artículo 18.4, que los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite.

En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes, no debiéndose facilitar información que afecte a la intimidad del fallecido, ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

En cuanto a las dudas surgidas –en materia de protección de datos- a raíz de las investigaciones en curso relacionadas con los supuestos de posibles **"robos de niños",** mi opinión más personal al respecto pasa por la aceptación de las siguientes máximas:

1.- Cuando oficialmente una persona figura como "fallecida" en los correspondientes registros oficiales (Registro Civil, archivos de hospitales y/o clínicas, registros de cementerios, etcétera), no cabría oponer –en ningún caso- el derecho a la protección de datos del "fallecido" como óbice para la correspondiente investigación. Esta interpretación debería resultar extensible a los supuestos del denominado "legajo de abortos", en el que –en el ámbito de los Registros Civiles- se inscriben los fallecimientos de los individuos que no gozan de la consideración civil de persona.

2.- El acceso a los correspondientes datos, solicitados generalmente por los padres y/o madres que –presuntamente- pudieran haber sido objeto de este tipo de ilícitos, se encontraría amparado legalmente en razón de lo dispuesto en la normativa sobre procedimiento administrativo común, y, especialmente por lo previsto en los artículos 31, 35 y 37 de la Ley 30/1992, de 26 de noviembre, que suponen un claro desarrollo del artículo 105 b) de la Constitución Española de 1978.

ACCESO POR LOS PADRES SEPARADOS QUE NO TENGAN LA CUSTODIA DE SUS HIJOS MENORES A LOS DATOS DE SALUD DE ÉSTOS

Para determinar la posibilidad de acceder a los datos de salud de los menores por parte de los padres separados que no tengan la custodia de sus hijos, debe acudirse a la legislación específica para el ámbito de la información en materia sanitaria que se encuentra en la Ley 41/2002, de 14 de noviembre, básica reguladora de "la autonomía del paciente".

Concretamente, el Capítulo II recoge las directrices a seguir para satisfacer el derecho de la información sanitaria, estableciéndose, en el artículo 5, que el titular del derecho a la información es el paciente, quien tendrá que ser informado, incluso en caso de incapacidad, de modo adecuado a sus posibilidades de comprensión, cumpliendo con el deber de informar también a su representante legal.

Asimismo, en el artículo 18 de la Ley 41/2002 dispone que es el paciente el que tiene derecho de acceso a la documentación de la historia clínica, y a obtener copia de los datos que figuran en ella, debiendo los centros sanitarios regular el procedimiento que garantice la observancia de esos derechos. Según este artículo, dicho derecho puede ser ejercido también por representación debidamente acreditada.

En los casos de padres separados será la resolución judicial la que determinará todo lo relativo a la patria potestad y a la guarda y custodia de los hijos, siendo normalmente ejercida por aquel con quien el hijo conviva (art. 156 del Código Civil), salvo que el juez determine otra cosa.

Como señala el artículo 162 del Código Civil, los padres que ostenten la patria potestad tienen la representación legal de sus hijos menores no emancipados. El ejercicio de la patria potestad es determinante para ostentar la representación legal de los menores y, por tanto, para acceder a todos los datos relativos a su salud, y la presentación del documento judicial que haga mención a la patria potestad y asignación de guarda y custodia deberá ser suficiente para acceder a la información asistencial de los menores. En con-

secuencia, a los padres o tutores de los menores se les considera destinatarios de la información asistencial de éstos.

La comunicación a los padres de los datos relativos a la información asistencial de sus hijos no puede considerarse cesión de datos del menor, siempre que ostenten la patria potestad y, por ende, su representación legal, sino que es una manifestación del ejercicio del derecho de acceso a datos personales por parte de los representantes legales del afectado.

Desde el punto de vista de la legislación de protección de datos, no existe ningún motivo que impida a un padre separado la solicitud de información asistencial de su hijo menor, es decir, el ejercicio del derecho de acceso a los datos de salud, siempre que ambos ostenten la patria potestad, condición que podrá acreditarse con la presentación del documento judicial que recoja lo relativo a la patria potestad de los progenitores. Éstos tienen el derecho de acceso a los datos de sus hijos menores en caso de ostentar ambos la patria potestad, en cuanto se erigen como sus representantes legales.

En consecuencia, los servicios sanitarios tienen la obligación de contestar los requerimientos de información sobre la salud de los hijos menores por parte de los padres separados, tantas veces como se produzcan (dentro de las condiciones y plazos aplicables), siempre y cuando los padres ostenten la patria potestad de los mismos.

TRATAMIENTO DE LOS DATOS DE SALUD DE LOS ALUMNOS CON DISCAPACIDAD PARA LLEVAR A CABO LAS CORRESPONDIENTES "ADAPTACIONES CURRICULARES"

La especial protección conferida a los datos relacionados con la salud de las personas no es arbitraria, sino que resulta de lo dispuesto en las normas internacionales y comunitarias reguladoras del tratamiento automatizado de datos de carácter personal (artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, Apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa y artículos 6 y 45 del propio Convenio 108, y Recomendación n.º R 97-5, adoptada por el Comité de Ministros del 13-II-1997, relativa a protección de datos médicos).

En este escenario, la información de los alumnos, cuando ésta contenga datos de salud relativos a trastornos y enfermedades padecidas por los mismos podrían –en su caso- justificar la existencia de "adaptaciones curriculares" determinadas a favor de aquellos.

En el artículo 7 de la LOPD (especialmente, en su apartado 3) se establece que la información más sensible, que afecta en mayor medida a la intimidad y privacidad de las personas y al ejercicio de los derechos fundamentales consagrados por la Constitución, sea objeto de una protección reforzada, que pasa, en la mayor parte de los supuestos, por la exigencia del consentimiento del afectado para su tratamiento.

En consecuencia, este tipo de datos, necesarios para llevar a cabo la "adaptación curricular" de los alumnos, sólo podrían comunicarse en caso de que así se hubiera consentido por los propios alumnos o su representante legal o cuando una ley lo dispusiera, siendo así que –de la normativa aplicable- no se desprende la existencia de una norma habilitadora para la comunicación de dichos datos.

Así, conviene aclarar que, de lo establecido en los artículos 71 y 72 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOE), no se extrae la existencia de habilitación alguna que dé cobertura al tratamiento inconsentido de los datos de salud de los alumnos. Esto es, la recogida, tratamiento y cesión inconsentida de datos de salud de las personas no encuentra amparo en la citada LOE, sin que resulte admisible que la mera atribución genérica de competencias, la descripción de funciones legales o la determinación legal de las obligaciones de los centros y/o del profesorado resulte suficiente para considerar válido el tratamiento inconsentido de dichos datos.

En conclusión, sin perjuicio de la obligación de "información" en la recogida de los datos (artículo 5 de la LOPD), en estos supuestos deberá procederse, en todo caso, a recabar el consentimiento expreso de las personas afectadas en relación con la recogida de sus datos de salud.

Asimismo, de conformidad con el artículo 4 de la LOPD, en el supuesto de que se facilitasen datos personales, siempre y cuando exista consentimiento expreso y previo para la comunicación de los mismos, los datos que se recaben deberán ser adecuados, pertinentes y no excesivos para la finalidad para la cual se recaban, debiendo ser cancelados o borrados cuando hayan dejado de ser necesarios para el fin que motivo dicha recogida.

Protección de datos de salud: casos prácticos de la experiencia de la Autoridad Catalana de Protección de Datos

Carles San José Amat
Jefe del Área de Inspección
Autoridad Catalana de Protección de Datos

A continuación se exponen una serie de casos prácticos que derivan de distintas denuncias y reclamaciones de tutela de derechos que se han presentado ante la Autoridad Catalana de Protección de Datos, todas ellas referidas al tratamiento de datos de carácter personal relativos a la salud.

DERECHO DE ACCESO A UNA HISTORIA CLÍNICA ILOCALIZABLE

Un ciudadano presentó una reclamación de tutela de derechos por la desatención de su derecho de acceso a la historia clínica. En concreto, se quejaba que el Hospital ante el cual había ejercido su derecho de acceso le había comunicado que no le podían facilitar su historial clínico por encontrarse éste ilocalizable. Tal circunstancia lleva a preguntarnos si justifica la denegación de la solicitud de acceso ejercida.

Pues bien, es evidente que entre las causas previstas en la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD) y en el Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante, RLOPD), que permiten denegar o modular el derecho de acceso, no se contempla la circunstancia relativa a la pérdida de la documentación, lo que lleva a preguntarnos lo siguiente:

¿Y de qué forma tenía que haber actuado el Hospital?

Tal como se ha avanzado, la pérdida de la historia clínica en formato no automatizado, es decir, en papel, no exime al responsable del fichero de facilitar toda aquella información que se pueda recuperar, ya sea porqué la información también se conserva en formato automatizado, o bien, porqué existen copias de la documentación en formato papel en otros ficheros o archivos.

Por lo tanto, con la finalidad de atender adecuadamente la petición de acceso ejercida, el Hospital debió haber llevado a cabo la tarea de reconstrucción de la historia clínica que se encontraba ilocalizable. Puesto que de los hechos descritos se podían inferir un eventual incumplimiento de la LOPD, se inició un procedimiento sancionador.

El Hospital alegó que una parte de la historia clínica se conservaba en formato papel, y la otra, en formato automatizado. Asimismo, ponía de manifiesto que las historias clínicas originales en formato papel se podían extraer del archivo, en cuyo caso se hacía constar en la correspondiente aplicación informática un identificador del lugar de destino.

En el presente caso, constaba en dicha aplicación que la historia clínica se había facilitado a un determinado servicio del Hospital 4 años atrás, sin que se tuviera constancia de la devolución de la historia clínica al archivo, por lo que no se podía determinar con certeza dónde se encontraba ésta.

Debe recordarse aquí que la jurisprudencia exige al responsable del fichero o el tratamiento que actúe con cierta diligencia, diligencia que en el supuesto de tratarse con datos relativos a la salud debe ser de mayor intensidad. Por este motivo, se sancionó al Hospital por no haber implementado las medidas pertinentes para garantizar la seguridad de los datos, y en especial, su pérdida.

En relación al deber de custodia de la historia clínica la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, impone una serie de obligaciones relativas a su conservación y custodia, tanto para garantizar el ejercicio del derecho de acceso (artículo 7.2) como la seguridad y recuperación de la información (artículos 14 y 17), en cuyo caso se remite a lo establecido en la LOPD (artículo 17.6).

Por otra parte, el artículo 17.1 de la Ley 41/2002, permite que no se conserve el original de la historia clínica. Es decir, abre la puerta a que dicha documentación se pueda conservar en otros formatos, como por ejemplo, en formato automatizado a través del escaneado.

CONSENTIMIENTO NO LIBRE

En otro caso que llegó a conocimiento de la Autoridad, un ciudadano denunció a la entidad encargada del control, inspección, avaluación y seguimiento en materia de incapacidades laborales, por el hecho de que la doctora que les atendió le exigió que se identificara mediante su

DNI. Concretamente, la persona denunciante exponía que ella simplemente acompañaba a la paciente que se tenía que visitar por una determinada doctora, quién exigió, sin motivo aparente y sin informarles, que ambos se identificaran mediante su DNI, bajo amenaza de no atenderles. Ante tal amenaza, ambas personas se identificaron, procediendo la doctora a fotocopiar su DNI.

En el marco de las actuaciones previas, la entidad denunciada admitió los hechos denunciados, si bien especificaba que, como es lógico, se requería a toda persona que debía ser visitada que se identificara al efecto de comprobar su identidad y poder realizar una correcta avaluación médica. Así, la identificación del paciente se encontraba totalmente justificada.

Ahora bien, en relación a la persona acompañante, la entidad denunciada admitió que no era necesario que éste se identificara, informando de tal extremo a la doctora implicada con la finalidad de que no se repitiera esta conducta.

En la valoración de los hechos se tuvo en cuenta el artículo 3.h) de la LOPD, que define el consentimiento como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen."* En el presente caso, si bien es cierto que la persona acompañante consintió el tratamiento de sus datos por parte de la doctora, este consentimiento no se prestó de forma libre, puesto que si no se entregaba el DNI la doctora amenazaba de no atender a la paciente que se tenía que visitar.

También es cierto que, según informó la entidad denunciada, el hecho de identificar al acompañante podía llegar a considerarse comprensible, ya que pocos días antes se había tenido conocimiento de una sentencia en que se absolvía a un acompañante que presuntamente habría amenazado a un médico, porqué en su momento no pudo ser identificado. Por este motivo, la entidad denunciada consideraba que esta circunstancia era un atenuante de su conducta.

En efecto, de haberse impuesto una sanción económica probablemente se habría graduado la sanción teniendo en cuenta lo alegado por la denunciada. No obstante lo anterior, es necesario recordar que en relación a las infracciones de las que sean responsables las Administraciones Públicas, la resolución se limitará a declararlas y a imponer las medidas que correspondan para que cese o se corrijan los efectos de la infracción. Es decir, en ningún caso se impondrá una sanción económica, de modo que no entran aquí en juego los criterios de graduación de la cuantía de las sanciones previstos en el artículo 45 de la LOPD, ni tampoco la solución del simple apercibimiento sin imposición de multa, posibilidad prevista en el art. 45.6 de la LOPD.

INFORMACIÓN TELEFÓNICA

Finalmente, un sindicato también denunció ante la Autoridad que un determinado centro hospitalario había establecido un protocolo para otorgar información a los familiares de los pacientes ingresados en la unidad hospitalaria penitenciaria. La denuncia se centraba en que se contemplaba la posibilidad de otorgar la información relativa al estado de salud de los pacientes por vía telefónica, vía que no consideraban bastante segura para garantizar la confidencialidad de los datos de los pacientes atendidos.

El protocolo en cuestión preveía que el paciente concretara, con carácter previo, la persona autorizada a recibir la información, así como que era necesario que el propio paciente fuera quien proporcionara el teléfono de contacto.

Lo primero que se resolvió en este caso fue que la simple aprobación del protocolo no conllevaba la comisión de infracción alguna, por lo que hasta que no se pusiera en aplicación no se podría entrar a dirimir si se había producido o no alguna infracción de la LOPD. Por este motivo, en el presente supuesto, no se consideró acreditado que el Hospital hubiera permitido que personas no autorizadas accedieran a la información de los pacientes atendidos en la unidad hospitalaria penitenciara.

Ello no obstante, es necesario recordar que el tratamiento de datos de carácter personal relativos a la salud, como datos especialmente protegidos, requiere el consentimiento expreso de la persona afectada. En el presente caso, esta circunstancia se salvaba pues el paciente firmaba una autorización consintiendo que se informara de su estado de salud por medio del teléfono a las personas que designara, facilitando a tal fin el número de teléfono al que se había de llamar.

En la resolución que se dictó en estas actuaciones se consideró que, si bien el uso del teléfono para informar acerca del estado de salud de un determinado paciente no es un medio que garantice de forma absoluta que la persona interlocutora sea la persona autorizada, lo cierto es que precisamente el paciente es quién ha facilitado ese número de teléfono concreto y quién lo ha autorizado. En cuanto a las llamadas que se recibían del exterior, la Autoridad Catalana de Protección de Datos sugirió que, en la medida que no fuera posible garantizar que la persona interlocutora era la expresamente autorizada por el paciente, lo más conveniente era no facilitar información relativa a la persona ingresada con motivo de llamadas entrantes, de modo que debía ser el propio Hospital quién efectuara la llamada al número de teléfono designado al efecto.

La mejora de la información clínica: una garantía para la seguridad del paciente

Manuel Gimbert [1], Ana Mª Chups [2] y Martín Tejedor[3]

1. Responsable de Seguridad de la Información. Servicio de Calidad y Documentación Clínica. Hospital Reina Sofía de Córdoba.

2. Jefe de Servicio de Informática. Hospital de la Merced de Osuna. Sevilla.

3. Jefe de Servicio de Calidad y Documentación Clínica. Hospital Reina Sofía de Córdoba

INTRODUCCIÓN

El título original de la 4ª sesión del IX FORO SOBRE PROTECCIÓN DE DATOS DE SALUD fue: "Mejores prácticas para la mejora de la seguridad: iniciativas y proyectos", sin embargo hemos preferido atrevernos a cambiar el título por el que aparece más arriba, ya que después de leer el artículo éste nos ha parecido más apropiado.

La LOPD[1] y el RD 1720/2007[2] han sido pilares fundamentales para el desarrollo de las políticas sobre seguridad de la información. Cuando se habla de protección de datos, se suele hacer referencia a la CONFIDENCIALIDAD. Se ha establecido un binomio **PROTECCIÓN DE DATOS - CONFIDENCIALIDAD** que se ha extendido entre los profesionales y que ha repercutido en la concienciación y en actuaciones relacionadas con el transporte y la custodia de las historias clínicas, por ejemplo.

Sin embargo, veremos a continuación que la verdadera inquietud entre los profesionales sanitarios no es la CONFIDENCIALIDAD, sino la **DISPONIBILIDAD** y sobre todo la **INTEGRIDAD** de la información.

Organismos como la Organización Mundial de la Salud (OMS) han establecido una relación directa entre SEGURIDAD DE LA INFORMACIÓN y SEGURIDAD DEL PACIENTE, hablando en términos de incidentes de seguridad y eventos adversos, pero sobre aspectos directamente relacionados con la información en cuanto a:

- Errores de identificación del paciente
- Errores de comunicación PROFESIONAL - PROFESIONAL
- Errores de comunicación PROFESIONAL - PACIENTE

Términos como "identificación" y "comunicación", parecen estar más cercanos al mundo de las tecnologías de la información y comunicación (TIC) que a la esfera de la sanidad.

El Estudio Nacional sobre los Efectos Adversos ligados a la Hospitalización, **ENEAS 2005**[3], incluye la **siguiente definición:**

Error por deficiente identificación.

Incluye todas las actuaciones realizadas a un enfermo para el que no estaban destinadas como consecuencia de una identificación deficiente (ej.: transfusiones a enfermo equivocado, errores en actuaciones quirúrgicas, miembro equivocado, etc.).

Además tipifica a los eventos adversos, como los siguientes:

- Retraso en el diagnóstico por falta de pruebas pertinentes (¿Disponibilidad de la información?)
- Error de identificación del paciente. (¿Integridad de la información?)
- Error de etiquetas identificativas en los tubos de hemograma. (¿Integridad de la información?)
- Transmisión incorrecta de los resultados de microbiología. (¿Integridad de la información?)
- Cirugía de sitio equivocado. (¿Integridad de la Información?)
- Confusión de la historia clínica. (¿Integridad de la información?)
- Letra ilegible en el informe de alta. (¿Integridad de la información?)
- Deficiente información sobre tratamiento post-alta. (¿Integridad de la información?)

Por otro lado, según la OMS, calcula que en los países desarrollados uno de cada 10 pacientes sufre algún tipo de daño durante su estancia en el hospital. Este porcentaje sube hasta el 12% si se trata de las urgencias en España (Informe EVADUR sobre eventos adversos ligados a la asistencia en los servicios de urgencias de hospitales españoles 4).

Una de las iniciativas más influyentes son los Objetivos para la Seguridad del Paciente que propone anualmente The Joint Commision 5, tratando de concentrar los esfuerzos en los aspectos considerados más prioritarios para la mejora de la calidad y seguridad de los centros sanitarios.

Entre los objetivos propuestos para el 2011 encontramos los siguientes:

Objetivo 1: Mejorar la identificación del paciente

- NPSG.01.01.01: Utilizar al menos dos identificadores del paciente cuando se proporcionan servicios, tratamientos y cuidados

- NPSG.01.03.01: Eliminar los errores en las transfusiones relacionados con la identificación del paciente.

Objetivo 2: Mejorar la comunicación efectiva entre cuidadores

- NPSG.02.03.01: Informar a tiempo y de manera oportuna sobre los resultados críticos de pruebas diagnósticas.

Objetivo 3: Mejorar el uso seguro de los medicamentos

- NPSG.03.04.01: Etiquetar la medicación, sus contenedores (jeringas, botes, etc.) y otras soluciones.

Objetivo 8: Asegurar la precisión de la medicación en las transiciones asistenciales

- NPSG.08.02.01: Cuando el paciente es transferido a otro hospital o a atención primaria, el listado completo y conciliado de medicación se comunica al siguiente proveedor.
- NPSG.08.03.01: Cuando el paciente abandona el hospital se le proporciona un listado completo y conciliado de la medicación, que se explica al propio paciente o a su familia.

En el Registro de eventos adversos en el Hospital Universitario Reina Sofía (HURS) se hicieron 409 notificaciones en el año 2011.

2 %– pegatinas erróneas en la historia clínica (DENTRO DE LA HISTORIA CLÍNICA)

9 % – mezcla de documentos en el sobre contenedor de la historia clínica.

4 % – falta de identificación en algunos documentos.

6 % – etiquetado erróneo.

Esto es un 21% del total de incidentes notificados en el HURS en 2011, relacionados con seguridad de la información (integridad).

Tampoco se nos puede pasar por alto el gran parecido de este registro de eventos con el registro de incidencias establecido por el RD 1720/2007 y no podemos dejar de hacernos una pregunta ¿Cuantos registros de incidencias LOPD tienen 409 registros?

En el Archivo de historias clínicas se detectan una gran cantidad de duplicados, de tal modo que un equipo de 7 personas tiene esto entre sus funciones y para fusionar las historias clínicas duplicadas detectadas. De nuevo falta en la INTEGRIDAD de la información. Adicionalmente hay que subrayar que esto no afecta sólo a la seguridad del paciente y la seguridad de la información, sino que este tipo de errores tienen un coste económico.

De la Protección de Datos a la Seguridad de la Información

El objetivo principal de la Seguridad de la Información consiste en garantizar la actividad de la organización a la que presta sus servicios. En nuestro caso, la prestación de los servicios Sanitarios a los ciudadanos. El cumplimiento legal, es uno de los items que hay que considerar, que por supuesto, es obligatorio y ni es negociable ni susceptible de priorización.

Sin embargo, parece claro, a la vista de los datos antes mencionados, que la verdadera preocupación de organizaciones y profesionales sanitarios no es la "protección de datos" en el sentido de "privacidad", ni el cumplimiento legal, sino que son la INTEGRIDAD y DISPONIBILIDAD y la **SEGURIDAD DEL PACIENTE.**

En esta tarea de "pasar de hablar de protección de datos a hablar de seguridad de la información", lleva el Servicio Andaluz de Salud varios años trabajando. En 2008 se formaron una decena de Certified Information System Auditors (CISA) y en 2012 ha comenzado a formarse una nueva promoción. En este mismo año han comenzado a formase 8 Certified Information Security Management (CISM).

Se han definido las políticas, normas y procedimientos corporativos generales desde la Unidad de Gestión de Riesgos Digitales del Servicio Andaluz de Salud (SAS), que forman el Documento de Seguridad de la Información corporativo y que cada centro adapta según sus particularidades.

No todos los riesgos inherentes a la información se resuelven a través de la tecnología. Un programa de concienciación sobre seguridad de la información puede reducir en gran medida los riesgos de seguridad al actuar incidiendo sobre la conducta de los profesionales

El Plan de Concienciación del SAS 2008 - 2012, ideado y coordinado también por la Unidad de Gestión de Riesgos Digitales, ha llegado ya a más de 70.000 profesionales del SAS de todas las categorías incluyendo al personal directivo. Más de 4.500 sólo en el HURS.

La formación específica ha sido dirigida a colectivos concretos: profesionales de Archivos de Historias Clínicas, de los Servicios de Atención al Ciudadano, de los Servicios de admisión, investigadores....., de forma que se establezcan procedimientos de actuación similares de forma transversal en toda la organización y se difundan por igual las políticas, normas y procedimientos corporativos a los colectivos profesionales.

Para contar con un referente adecuado, que actúe como asesor a la organización es necesaria la figura del "Responsable de Seguridad de la Información" que además es obligatoria según la Ley Orgánica de Protección de Datos (LOPD).

Para añadir verdadero valor a la organización, el responsable de Seguridad de la Información debe dedicarse a tiempo completo a esta función y ser independiente de los Servicios de Tecnologías de la Información que limitan sus funciones y un trabajo objetivo independiente. El responsable de Seguridad debe informar y asesorar a la dirección, de forma directa y/o a través de una Comisión de Seguridad de la Información.

Tal y como exigen todos los estándares internacionales y desde enero de 2010 el Esquema Nacional de Seguridad, el HURS mantiene el principio de **"separación de roles",** de forma que las distintas figuras que intervienen en el tratamiento y seguridad de la información se mantienen independientes.

Otra herramienta fundamental es la **Comisión de Seguridad de la Información.** Su misión consiste en impulsar el proyecto de adecuación a la LOPD del centro. Pero sus funciones van mucho más allá:

- Apoyando e impulsando los planes de seguridad nacidos de las sucesivas auditorías.
- Asesorando a la Dirección Gerencia del Centro en lo que respecta a seguridad de la información
- Garantizando la alineación de los objetivos de seguridad de la información con los objetivos de la organización (seguridad del paciente)
- Coordinándose con otras comisiones relacionadas, como la de seguridad del paciente y la de historias clínicas.

Por otro lado, con la participación del Responsable de Seguridad de la Información en la **Comisión de Seguridad del Paciente s**e trata de garantizar la alineación de los objetivos de seguridad de la información con los objetivos de seguridad del paciente y por extensión de la organización, una más de las preocupaciones de los centros sanitarios. No debemos olvidar que nuestra razón de ser son los pacientes y, por tanto, cualquier actividad en materia de seguridad de la información debe estar directamente orientada a la mejora de la asistencia que se les presta, apoyándose para ello, por supuesto, en sus pilares fundamentales, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD de la información.

En 2008 el Hospital Reina Sofía se sometió a una auditoría externa de la cual se derivó el primer plan de seguridad de la información del centro. En 2010 se realizó una autoevaluación interna sobre los niveles de cumplimiento de la LOPD, de la cual se ha derivado el segundo plan de seguridad de la información del hospital.

Desde finales de 2010 el Servicio de Calidad ha realizado 13 auditorías internas a nivel de Unidades de Gestión Clínica y están previstas otras 6 para el 2012.

Un **programa de seguridad de la información** comprende todas las actividades y recursos que proporcionan servicios de seguridad de la información a una organización.

El HURS llevó a cabo el primer programa de seguridad de la información entre 2010 y 2012, Y aunque aún nos quedan asuntos pendientes que mejorar respecto del primer plan de seguridad de la información, ya hemos puesto en marcha el segundo para el periodo 2012-2014.

Como conclusión, diremos que hay que pasar de hablar sobre **"protección de datos"** al concepto más amplio de **"seguridad de la información"** en el marco de la **"seguridad del paciente"** teniendo muy en cuenta, que cualquier objetivo de seguridad de la información debe estar orientado y ser coherente con los de la organización.

En la medida en que seamos capaces de alinear las actividades de seguridad de la información con las de seguridad del paciente, será más fácil para las organizaciones y los directivos entender la importancia de los planes de seguridad de la información, las consecuencias "clínicas" de descuidar la integridad, disponibilidad y confidencialidad de la información y el papel que juegan las leyes sobre protección de datos y seguridad de la información en la defensa de la prestación de servicios sanitarios de calidad y en la salud de los ciudadanos.

BIBLIOGRAFÍA

1. **LEY ORGÁNICA 15/1999,** de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm. 298, de 14 diciembre 1999.
2. **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. BOE núm. 17, de 19 enero 2008.
3. **Aranaz JM, Aibar C, Vitaller J, Ruiz P.** Estudio Nacional sobre los Eventos Adversos ligados a la Hospitalización. ENEAS, 2005. Madrid: Ministerio de Sanidad y Consumo, 2006.
4. **Tomás S, Chanovas M, Roquetas F, Alcaraz J, Toranzo T y Grupo de Trabajo EVADUR-SEMES.** EVADUR: eventos adversos ligados a la asistencia en los Servicios de urgencias de hospitales españoles. Emergencias 2010; 22: 415-428.
5. **National Patient Safety Goals.** Disponible en http://www.jointcommission.org/standards_information/npsgs.aspx.

La seguridad, las estrategias y la ortografía

Juan Miguel Signes Andreu. CISA, CISM
Responsable de seguridad de la información. Conselleria de Sanidad y Agencia Valenciana de Salud. Generalitat Valenciana

Seguridad se escribe con eñe, con eñe de ...ñazo (complete a su gusto la línea de puntos). Esta sentencia, a mitad camino entre el aforismo y el chascarrillo, se nos hace muy presente cuando nos toca sufrir las restricciones o incomodidades impuestas en nombre de la seguridad, sea a la hora de pasar los controles de viajeros de un aeropuerto, o a la de recordar la contraseña de acceso a nuestra Wi-Fi doméstica, por no hablar de los preservativos.

En tales ocasiones pensamos que la vida sería mucho más fácil sin todo ese fárrago de controles, aseguramientos y verificaciones. Si bien eso es cierto, no lo es menos que el mundo es como es, o como lo hemos hecho, y que asumir determinados niveles de seguridad y de riesgo es algo inherente a cualquier actividad. La cuestión está en decidir las proporciones, y en quién puede o debe tomar esa decisión. El acierto en estas decisiones tiene mucho que ver con el éxito o el fracaso de la actividad en cuestión.

Nunca hasta ahora la actividad de las organizaciones ha dependido tanto de la información y de sus tratamientos. Aunque sólo fuera por este motivo la necesidad de plantear la seguridad de la información a escala corporativa ya estaría justificada. En otras palabras, que ocuparse de la seguridad de la información es hoy en día un deber para las organizaciones, y por motivos de mera supervivencia. Así, con el futuro de la organización en juego, los máximos directivos tienen que jugar un papel importante en este asunto de la seguridad.

A pesar de las noticias que llegan a las portadas de los diarios y que ilustran lo expuesto en el párrafo anterior, llama la atención que todavía haya directivos que piensen que la seguridad de la información no va con ellos, que es cosa de un departamento especializado, de sus informáticos, de un proveedor externo que monitoriza el funcionamiento de la red corporativa, o de los letrados que redactan los contratos. Afortunadamente para esos directivos la seguridad de la información no sólo es un deber, sino también una exigencia legal, y el cumplimiento de estas obligaciones viene a recordar sus deberes a quienes no fueran demasiado conscientes de ellos.

Una segunda característica de la normativa legal es que ahorra algunas decisiones al exigir, con carácter de mínimo, la aplicación de unas medidas de seguridad concretas para manejar determinados tipos de información. Ambas características son buenas noticias, desde luego, pero quien pretenda cubrir sus necesidades de protección fijándose sólo en el cumplimiento legal podrá esquivar alguna multa, pero perderá el rumbo y seguramente algo peor.

El conocimiento de la organización, de la actividad que desarrolla, y de su grado de dependencia de la información y de los sistemas de tratamiento es insustituible a la hora de dirigir las actuaciones en seguridad. Esto es lo que algunos llaman alineamiento con los objetivos de la organización, y plantear la seguridad de la información en estos términos proporciona numerosas ventajas.

La primera ventaja y la más evidente es poner la seguridad al servicio de la organización. Y es que la seguridad puede aportar mucho a las organizaciones, incluso antes de que ocurra un incidente o un desastre que justifique las inversiones realizadas. Este valor es, con frecuencia, el papel de catalizador que puede jugar la seguridad en la transformación de las organizaciones hacia niveles superiores de madurez en el desempeño de sus actividades. La necesidad de establecer procedimientos, documentarlos y someterlos a control y mejora continuos tienen mucho que ver con esa transformación. El resultado no son solo organizaciones más seguras, sino también más maduras, capaces de ofrecer productos y servicios de mayor calidad.

La visión de la seguridad expuesta en el párrafo anterior podría parecer fruto de un arrebato ingenuo y voluntarista de un empleado apasionado, o un extracto de la carta de presentación de una empresa especializada en servicios de consultoría de seguridad. Podría ser, pero lo cierto es que esa visión es precisamente la que exigen la normativa sobre protección de datos personales y el esquema nacional de seguridad a las instituciones sanitarias de nuestro sistema nacional de salud.

Una vez enfocado el problema, lo siguiente es decidir por dónde empezar. Sin ánimo de dar lecciones a nadie, a continuación expondremos algunos aspectos principales de la estrategia que estamos siguiendo en la Conselleria de Sanidad de la Generalitat valenciana.

SEGURIDAD DE LA INFORMACIÓN

El primer paso debe darlo la alta dirección afirmando su compromiso con la seguridad, que como hemos visto equivale a responsabilidad y diligencia en el funcionamiento de la organización, así como en la protección de los intereses vinculados a la información objeto de tratamiento. El mejor modo de hacer público este compromiso es aprobando una política de seguridad de la información.

La política debe ser un documento de carácter público con dos destinatarios claros. En primer lugar los ciudadanos en general, para informarles de los principios y de los controles de seguridad que se aplicarán en todos los tratamientos de información. La política debe transmitir confianza en el modo en que la organización maneja la información, especialmente si se trata de datos personales. Evidentemente este documento no puede quedarse en una declaración de buenas intenciones, y por eso su segundo destinatario es el personal al servicio de la organización: los compromisos con los ciudadanos se convierten así en obligaciones para los trabajadores, incluidos los de las empresas contratadas, becarios, voluntarios, etc.

Un ejemplo reciente de este tipo de documentos es la Política de seguridad de la información de la Generalitat valenciana (http://www.docv.gva.es/datos/2012/04/30/pdf/2012_4162.pdf).

La Política es un documento de alto nivel que marca un rumbo, pero que debe concretarse más para facilitar su aplicación en la práctica real. El nivel de detalle adicional lo aportan tres colecciones de documentos: las normas, los procedimientos y las guías de buenas prácticas. Las normas se centran en actividades concretas y mantienen cierto nivel de generalidad. Los procedimientos describen las secuencias de pasos necesarios para completar una tarea. A diferencia de las guías de buenas prácticas, las normas y los procedimientos tienen carácter obligatorio.

TAREAS Y RESPONSABILIDADES

La política carecería de credibilidad por sí sola si no se acompañara de un inventario mínimo de tareas y su correspondiente asignación a distintos agentes dentro de la organización. Este documento conviene que sea público, pero va dirigido sobre todo a quienes trabajan al servicio de la organización. En organizaciones grandes o complejas conviene separarlo de la Política porque ambos documentos pueden tener vida propia.

El número y tipo de agentes con funciones específicas en seguridad de la información pueden variar mucho de una organización a otra. Los principios rectores más importantes son la eficacia y la separación de funciones entre los responsables de la seguridad, de la información y de los tratamientos. A partir de aquí hay margen para la creatividad, teniendo en cuenta también el mapeo con los agentes que exige la normativa aplicable.

El control, la evaluación y la mejora continua son factores clave también en el reparto de tareas y responsabilidades. Si determinado modelo organizativo, o determinados agentes no funcionan como sería deseable, se cambian por otros. Hay que tener en cuenta que normalmente sólo una exigua minoría de agentes tendrá dedicación exclusiva a la seguridad, por lo que el recambio será relativamente fácil. Las personas que mejor pueden desempeñar el papel asignado son la mejor opción, por encima de otras consideraciones.

INVENTARIO DE ACTIVOS

El tercer elemento imprescindible lo constituye el inventario de activos, que deberá distinguir entre activos de información y sistemas de tratamiento. Por activo de información se entiende cada conjunto de información con entidad diferenciada. Los ficheros declarados a la agencia de protección de datos son excelentes candidatos a ser considerados activos de primer nivel

Los sistemas de tratamiento son los conjuntos de elementos de distinto tipo (personas, datos, procedimientos, recursos...) que intervienen de manera coordinada en un tratamiento para hacerlo posible. Cuando entre tales elementos figuran las tecnologías de la información y las comunicaciones cabe hablar de sistemas de información.

La distinción entre activos de información y sistemas de tratamiento resulta esencial para identificar a los agentes con competencias sobre unos y otros, respetando así el principio de separación de funciones que exige el Esquema nacional de seguridad y recomiendan las buenas prácticas en la gestión de la seguridad de la información (véase la norma ISO/IEC-27002).

La identificación entre sistemas de información y ficheros de datos personales resulta poco afortunada, sobre todo si se trata de ficheros de titularidad pública y la responsabilidad sobre los mismos recae en el titular del órgano prestador de servicios sanitarios de una comunidad autónoma. De hecho, actuar de este modo obligaría a mantener el inventario de sistemas de tratamiento en el Registro general de protección de datos, previo paso por el diario oficial correspondiente por el procedimiento requerido para una disposición ordinaria. Una alternativa más razonable consiste en dar una interpretación genérica al concepto de fichero, establecer un estricto control inter-

no de los sistemas de tratamiento y vincularlos a los ficheros a través de sus correspondientes documentos de seguridad. Así, los documentos de seguridad cobran vida y se convierten en piezas clave del sistema de gestión de la seguridad.

MEJORA DE LA SEGURIDAD

Los elementos anteriores no dejan de ser descripciones o declaraciones bastante estáticas, y es preciso pasar a la acción. Las actuaciones a realizar vendrán dadas por los objetivos de la organización, las evaluaciones de riesgos y los resultados de las auditorías. Puesto que los recursos son limitados y no es posible hacerlo todo a la vez, resultará imprescindible concretar y priorizar las actuaciones, dotarlas de presupuesto, asignarlas, programarlas, etc. El resultado será el Plan de mejora de la seguridad.

Estos documentos contienen una planificación de alto nivel, a tres años vista, en la que las actuaciones concretas se alinean alrededor de unas pocas líneas de actuación principales. El objetivo de estas líneas de actuación es hacer frente a los principales problemas. Entre las líneas de actuación de cualquier Plan hay una que debe estar siempre presente: la sensibilización y formación del personal. Las actividades de sensibilización tienen carácter general y van dirigidas a todo el personal, mientras que las formativas van orientadas a colectivos específicos con necesidades muy concretas. En todo caso, mientras el personal que participa en los tratamientos de la información, o el que simplemente tenga acceso a los locales y sistemas donde se realizan, no sea consciente de su papel en el mantenimiento y la mejora de la seguridad, no vale la pena hacer grandes inversiones en tecnología y equipamiento de seguridad.

Otra característica importante de estos planes es que las actuaciones deben estar controladas de modo que permitan evaluar el grado de aplicación y la eficacia de las medidas de seguridad implantadas. Este es un requisito importante para poner en marcha los ciclos de mejora y las prácticas de auditoría continua. Así, abandonando planteamientos reactivos de la seguridad, con aproximaciones holísticas como la esbozada en los párrafos anteriores, intentando que la seguridad aporte valor a la organización, con esfuerzo, entusiasmo, colaboración y la justa dosis de suerte, tal vez consigamos olvidarnos de la eñe cuando hablemos de seguridad.



SEGURIDAD: Beneficios 360º

José Manuel Laperal González
Responsable de Seguridad e Innovación. Dirección General de Sistemas de Información Sanitaria. Servicio Madrileño de Salud

El ciudadano está cada día más despierto. Conoce ya bien sus derechos y le saca beneficios a la protección de datos. Hace unos años, nadie se planteaba nada en relación a los datos que un ciudadano otorgaba a las autoridades sanitarias. Los datos estaban ahí (o no estaban), ellos los tenían y te curaban. Casi ni pensabas en lo que el centro sabía o no de ti como paciente, se lo contabas tú y listos.

Hoy ya no es así, los ciudadanos empezamos a demandar que el centro sepa cosas de ti. Qué comodidad cuando te dicen: *"Ya veo que te hiciste la última prueba en julio y el resultado fue normal (menos mal que lo tienen porque se me había olvidado traer los resultados)!".* Cuestiones sobre cuántas cosas sabe el centro y cuantas no, sencillamente no se planteaban.

Hoy en día ya no es así. Nos preocupa que nuestras dolencias sean privadas, nos preocupa si ingresamos en un centro alguien sepa según qué cosas. Hasta ya nos empieza a preocupar que una persona pregunte en un mostrador y le digan en qué planta estamos ingresados. Ya no nos gusta tanto, o por lo menos no a todo el mundo esto le es indiferente.

Este tipo de medidas de protección cada vez son más demandadas. Empezaron con casos de personas bajo algún tipo de protección especial, o por tener intimidad frente a compañeros de trabajo, pero cada vez más son las personas que prefieren que no se ofrezca información sobre su salud ni siquiera en los mostradores de información.

De no interesar el tema de la protección de sus datos, hasta demandarla con interés ha transcurrido todo un largo camino. Adaptar los sistemas de información para hacerlos más seguros ha supuesto grandes inversiones, pero no solamente el ciudadano ha salido beneficiado sino que también el centro ha obtenido unos beneficios importantes. Muy importantes.

Por un lado el profesional sanitario se encuentra más protegido. En los tiempos que corren, los profesionales entienden que no exista libertad para acceso a las historias clínicas más allá de las necesidades de asistencia. Empezando por su propia intimidad, que no debe de estar a disposición de sus compañeros, y continuando por su protección en situaciones conflictivas en las que se demandan que se tenga la capacidad de discernir entre la diversidad de accesos, justo aquél acceso que es el único indebido y no se extienda la responsabilidad a toda una unidad, servicio o departamento.

El centro también empieza a obtener una información de alto valor. Por ejemplo, del análisis de los informes de consultas a pruebas diagnósticas, puede deducirse si está suficientemente justificado que crezca el ratio de solicitud de nuevas pruebas. En casos en los que no lo esté a nuestra satisfacción, podemos solucionarlo con una mejora en los procedimientos o protocolos, con una mejora en la formación en las herramientas existentes (lo que mejor aplique a la situación).

Con esto el centro ahorra tiempo y recursos para satisfacción de todos (sobre todo del paciente, al que no se las repiten). Son beneficios 360º, desde todos los puntos de vista.

Puestos a ello, a los responsables de un centro sanitario les interesará saber muchas más cosas, por ejemplo:

> *¿Porqué la actividad de consultas desde Atención Especializada a informes con antecedentes clínicos de Atención Primaria supone un x% menos desde los últimos dos meses?.*
>
> *¿Por qué este conjunto de datos casi no se consultan en esta tipología de centros?¿Es que son irrelevantes, o no hemos conseguido presentarlos de la forma adecuada para que sean útiles?¿Falta formación quizá?*
>
> *¿Podemos crearnos un mapa de visionado para saber qué se está consultando y desde dónde?*

Todo éste conocimiento de alto valor añadido y evidente interés, no es posible obtenerlo si no es por la aplicación de sistemas de auditoría sobre las consultas de acceso a los sistemas y guardar una adecuada trazabilidad de las mismas. Qué casualidad, justo lo que dice la LOPD que tenemos que hacer.

Convencidos, entonces. Explotamos la trazabilidad. Espera, pero, ¿antes o después de lo de modernizar el CPD? ¿Y la revisión del plan de contingencia entre medias, no? ¿Qué es lo más importante, cómo priorizamos?

La visión sobre la seguridad es una también la de una visión de 360º, desde distintos puntos de vista. Un centro efectivamente, se encuentra sometido a la necesidad de realizar una gestión de la seguridad desde diferentes enfoques y perspectivas. Es por tanto necesario disponer de una foto única que incluya todos los parámetros e interrelacione todos los indicadores de medida.

Esta visión global es otro de los beneficios porque aún más, en estos tiempos en los que cada euro cuenta tanto, es necesario tener una visión clara del resultado y mejora obtenida tras la inversión.

Éste siempre ha sido un problema clásico en las inversiones de seguridad, se abordaban proyectos que si bien mejoraban localmente una carencia en concreto, nos daban después la sorpresa de que no mejoraban la situación de conjunto, no hacían avanzar significativamente. Muchas organizaciones comprobaban con desconsuelo que después del gasto realizado en el último año en un sistema de identificación de usuario más ágil, no habían mejorado en otros aspectos que quizá más críticos, permanecían inmaduros, con lo que en el resultado final no se encontraban con una mejora significativa.

Para resolver esto es necesario ofrecer una visión de la seguridad (integral como hemos comentado antes) qué basada en los riesgos, muestre la situación en conjunto y permita obtener simulaciones de resultados, para poder decidir cuáles son las mejores inversiones, las que más nos hacen avanzar o resuelven aspectos más críticos.

En esta visión de la seguridad que queremos construir debe incluirse el impacto que la no existencia de la medida, causa en la organización. En el ámbito sanitario "¡todo es máximo!", por lo que nos generamos automáticamente un problema a la hora de priorizar, y como estamos acostumbrados a que todo es prioritario pues nos metemos en un círculo. Y la costumbre es siempre un mal compañero de viaje en la gestión de la seguridad. Perdemos sensibilidad sobre el alcance del riesgo cuando nos acostumbrábamos a él. Es un gran reto lograr que no sea así. Una buena receta, de las que funcionan siempre, es medir el riesgo, y pensar en la medida. Que no nos suene trivial, porque no lo es tanto cuando no siempre se hace. Si identificamos bien el impacto de un riesgo y pensamos en la medida que puede resolverlo o paliarlo, aunque no podamos aplicarla por el motivo que sea (económico, de alto impacto organizativo, etc.), al tenerla identificada hay muchas cosas que a partir de ahí podemos hacer. Aquí van dos breves ejemplos:

- La primera de ellas trasladar el riesgo, o por lo menos hacer partícipe a la organización del mismo. Con esto, no solamente habremos hecho algo que se espera de nosotros, sino que podremos presentarlo de forma comprensible y acompañado de una solución, si no totalmente detallada, cuando menos sí esbozada. Si esto nos parece obvio, revisemos sinceramente todos los riesgos que conocemos, y lo que nuestra organización conoce de cada uno de ellos. Y sobre todo, pensemos en la cara que se nos quedaría si escuchamos "si me hubierais dicho que por tantos-pocos-mil euros, esto no me pasaba, claro que lo habría autorizado!". "Pero si se lo dije mil veces y lo sabía todo el mundo que algún día esto iba a pasar!". En los malos momentos ya nadie sabe nada y todos se ponen de perfil. Revisemos por tanto, cómo estamos presentando la necesidad, asegurémonos que lo estamos haciendo de forma suficientemente gráfica y clara, y que la estamos acompañando del planteamiento de una solución con un alcance concreto y coste estimado.

- Dividir el problema en trozos más pequeños. Esta clásica recomendación aplica muy bien en el ámbito de la seguridad TI, por dos motivos. Por un lado es obvio que podemos identificar componentes de la solución que sean más asequibles de abordar, frente a presentar un gran TODO, mucho más complejo y para el que nunca encontramos ocasión y dinero. Esto además, nos ayuda por otro lado a presentar de una forma más responsable y profesional las necesidades. Es decir, cuando presentamos el problema, es altamente recomendable que las medidas que nos cuesten poco esfuerzo o dinero (realizar un procedimiento o plan, formación interna, etc), ya hayan sido realizadas y por tanto no exista esa vía de escape para nuestro "sponsor". "Cuando hayas hecho esto me vuelves a ver", ya no nos lo puede decir. Y frente a esto en ese momento nuestra frase podrá ser "lo que podía hacerse ya se ha hecho, lo barato ya se ha hecho, ahora lo que queda como siguiente paso es esto y cuesta tanto".

Con un planteamiento así de maduro y completo, nadie nos va a negar el apoyo que necesitamos.

Ética en la creación y gestión de biobancos: problemas y soluciones en red

Antonio Casado da Rocha
Departamento de Filosofía de los Valores y Antropología Social. UPV/EHU

RESUMEN

Los biobancos son herramientas para la investigación biomédica que albergan grandes cantidades de muestras y datos sanitarios, y a menudo en forma de redes de carácter internacional. Su novedad y complejidad generan problemas éticos y jurídicos que han obligado a replantear la justificación y condiciones del proceso de consentimiento informado. Aunque los comités de profesionales y expertos juegan un papel crucial en la gobernanza de estas infraestructuras, es deseable incorporar la perspectiva de los donantes y pacientes.

PALABRAS CLAVE

Biobancos, Comités, Ética de la Investigación, Autonomía, Consentimiento Informado

Las cuestiones éticas en la investigación biomédica se dan en un complejo escenario cuyos vértices son los profesionales sanitarios, los pacientes y usuarios del sistema, y la propia sociedad que financia y regula la investigación. Durante la última década, en ese triángulo se ha hablado mucho de biobancos, una clase de recursos definida en España por la Ley de Investigación Biomédica (2007) como el "establecimiento público o privado, sin ánimo de lucro, que acoge una colección de muestras biológicas concebida con fines diagnósticos o de investigación biomédica y organizada como una unidad técnica con criterios de calidad, orden y destino" (art. 3.d). En este artículo señalaremos brevemente algunos aspectos sobre la conveniencia de acercar los tres vértices del triángulo mediante prácticas adecuadas de información a varios niveles para que la creación y gestión de biobancos no genere problemas éticos y jurídicos. A tal fin, comentaremos algunos datos del último Eurobarómetro sobre estas cuestiones.

Resultado de la convergencia entre ciencias que han avanzado mucho en poco tiempo, como la genómica y la bioinformática, esta nueva tecnología aún está rodeada de mucha confusión, tanto a nivel técnico como ético y jurídico. Aunque la creación (noviembre del 2010) y el mantenimiento de la Red Nacional de Biobancos (www.redbiobancos.es, con 63 instituciones en 15 comunidades autónomas) supone un importantísimo avance en la materia, parte de esa confusión tiene su origen en el mismo carácter internacional de estas infraestructuras. La investigación en genómica se ha caracterizado por la sucesiva creación de plataformas de colaboración a varios niveles (regional, nacional e internacional) para compartir datos y prácticas. Este trabajo en red supone gobernar una gran diversidad en las definiciones y directrices, algo que no se puede obviar fácilmente en la investigación biomédica, que por su carácter traslacional debe mover información entre los centros asistenciales, los de investigación y los de desarrollo industrial.

En este panorama, respetar y proteger la autonomía informativa de los usuarios del sistema sanitario (o los sujetos fuente de investigaciones biomédicas) sigue siendo algo problemático para los profesionales que los atienden. El conocimiento de la legislación vigente, incluyendo la Ley de Autonomía del Paciente (2002), es limitado entre la población tanto lega como profesional. Podría decirse que tenemos un derecho sanitario avanzado pero que no ha terminado de impregnar la cultura bioética de nuestros centros asistenciales. Sin embargo, prestar atención a los aspectos éticos puede ahorrarnos que los problemas acaben en la vía jurídica. Lo inicialmente barato a veces sale caro, como pudo comprobar la Arizona State University cuando tuvo que pagar 700.000 dólares a los Havasupai, el grupo de indígenas americanos que la llevó ante los tribunales. Como relata el New York Times (23 de abril de 2010), la universidad obtuvo sus muestras para estudiar la diabetes, pero utilizó el biobanco en investigaciones sobre esqui-

zofrenia y los ancestros de los Havasupai, finalidades que no habían sido autorizadas por ellos.
La enseñanza es clara y de aplicación universal: los derechos de los participantes en una investigación son infringidos cuando no se les informa de manera comprensible y continua acerca del uso del material biológico que han donado a un biobanco. Se tarda menos y sale más barato hacer las cosas bien. Y para hacer las cosas bien hay que conocer mejor el contexto social en el que se implantan las innovaciones en ciencia y tecnología, especialmente en este ámbito de la investigación biomédica, donde la colaboración de la sociedad es vital ya que los científicos no sólo necesitan reconocimiento y financiación, sino sobre todo la cooperación y la confianza de sujetos de investigación dispuestos a donar parte de su material biológico.
Esto ya se vio desde los primeros casos relacionados con biobancos, como el de la ya famosa empresa deCODE genetics, cuya legislación (aprobada en 1998) incluía un tratamiento del consentimiento informado que fue declarado inconstitucional 5 años después. Desde entonces han proliferado los biobancos, impulsados por un conglomerado de intereses competitivos en la investigación biomédica, la industria farmacéutica y la política científica. Esta proliferación ha puesto en crisis los marcos regulatorios existentes, que no pueden adaptarse rápidamente a la evolución de la biomedicina y la fluidez de las sociedades en las que actúa, pero las experiencias islandesa y posteriores (como la británica del UK Biobank, www.ukbiobank.ac.uk) han dejado manifiesta la necesidad de informar e involucrar a la población desde las primeras fases del establecimiento de un biobanco.
Lo anterior viene a decir que, sea cual sea el marco legal, la participación de los legos no es un paso más en el establecimiento de un biobanco, sino parte integral de su gobernanza. Naturalmente, hay que reforzar la estandarización y armonización de procedimientos para que los biobancos puedan compartir recursos técnicos y éticos mediante guías de buenas prácticas. Para ello contamos con un precedente en la BBMRI (Biobanking and Biomolecular Resources Research Infrastructure), pero esta estructura de coordinación paneuropea reconoce dificultades a la hora de armonizar requisitos legales de sus 30 estados miembros. A esto se añade la inevitable diversidad en las actitudes sociales hacia la investigación biomédica y en las interpretaciones de la legislación europea.
Para valorar esa diversidad, y reconociendo el valor estratégico de los biobancos, la Comisión Europea incluyó en un reciente Eurobarómetro un estudio sobre percepción pública de estas infraestructuras (Gaskell et al. 2010). Las cifras más generales indican que uno de cada tres europeos había oído algo sobre biobancos y aproximadamente la mitad afirmaron que participarían en uno.
Fijándonos en países en concreto, uno de los datos más significativos es que sea precisamente en Islandia, el país que ha tenido mayor polémica y discusión pública sobre biobancos, donde la población exprese una mayor disponibilidad a donar muestras (el 54% aceptaría participar en un biobanco sin dudarlo, el 93% participaría probablemente). También es interesante comprobar que la idea de ceder cierta clase de información a un biobanco no provoca gran preocupación a la población en general. Si nos fijamos en los datos referidos a España (ver **Tabla 1**), sólo un tercio de los ciudadanos españoles declara estar preocupados por esa posibilidad, ya sea en lo referido a muestras de sangre, a tejidos procedentes de intervenciones quirúrgico-médicas, a datos de perfil genético, al historial clínico, o a información sobre su estilo de vida (datos sobre hábitos dietéticos, de ejercicio, etc.).
Ante estos datos, puede decirse que el contexto es-

TABLA 1. NIVEL DE PREOCUPACIÓN EN ESPAÑA POR LAS POSIBLES DONACIONES A UN BIOBANCO

(% de respuestas preocupadas por cada clase de información)

Muestras de sangre	35
Historial clínico	33
Perfil genético	32
Tejidos procedentes de intervenciones quirúrgico-médicas	31
Datos sobre estilo de vida (dieta, ejercicio,…)	26

Fuente: Eurobarómetro 73.1 (Gaskell et al. 2010, p. 63).

pañol sigue siendo favorable a la investigación biomédica (según datos del Eurobarómetro, España registró en el período 1991-2005 el mayor índice de optimismo ante la biotecnología en toda la Unión Europea). Con todo, un tercio de personas preocupadas por los biobancos no es un porcentaje a desdeñar. ¿Quién debe responsabilizarse de garantizar que se tiene en cuenta el interés general y la salud pública en la gestión y creación de biobancos? Si atendemos al Eurobarómetro hay una cierta división entre países que optan por una ética basada en la autorregulación de los profesionales involucrados, por un lado, y por el otro países que optan por regulación externa (incluyendo los CEI, Comités de Ética de la Investigación). En general, en los países con mayor apoyo a los biobancos (por ejemplo, en toda Escandinavia) se tiende a la regulación externa, mientras que en España se tiende a favorecer más la autorregulación. Podría decirse que la tendencia europea es hacia la regulación externa, aunque nuestro punto de partida sigue siendo la delegación de la toma de decisiones en manos de científicos y expertos.

Si nos centramos en uno de los temas que más polémica han generado, el del consentimiento informado para la cesión y utilización de muestras (cuestión clave en el caso de los Havasupai), siete de cada diez ciudadanos europeos optan por autorizar específicamente cada proyecto de investigación que utilice su muestra, y dos de cada diez optan por el consentimiento amplio (pero esta proporción sube hasta 4/10 en el subgrupo más dispuesto a participar en biobancos). Aquí no tenemos espacio para entrar en este problema del consentimiento informado (véase Casado 2011 para una aproximación al tema en un artículo de acceso libre). Baste decir que a nivel global se mantiene el modelo tradicional de consentimiento informado como una de las principales salvaguardas éticas de la investigación, cuya justificación se relaciona a su vez con la protección de la autonomía de los sujetos fuente. Hay un creciente consenso en torno a la idea de que no basta con ejercer esa autonomía en el momento de obtener el consentimiento, generalmente mediante una firma en un formulario. Por otro lado, no estamos hablando sólo de autonomía individual, ya que la investigación genética afecta a grupos humanos enteros. El consentimiento informado en este contexto requiere la participación continuada y la capacitación activa de los pacientes, donantes y otros sujetos que participan en la investigación, porque la autonomía es algo más que la capacidad de entrar o salir de un proyecto de investigación por medio de una firma Dado el papel crucial que asumen los CEI en el modelo de gobernanza español, a ellos corresponde verificar que ese proceso de información se dé en los proyectos de investigación que autorizan y supervisan. ¿Podrán hacerlo solos?

La relación entre confianza pública y participación de los donantes está bien estudiada en otros países. Hay un creciente consenso sobre la viabilidad, tanto en términos técnicos como éticos, de un planteamiento abierto en que los participantes son informados más allá del momento en el que se recabe su consentimiento para donar una muestra, pero nos falta implantar esos mecanismos de información interactiva. La informática sanitaria puede ayudar mucho en esa tarea, aumentando no sólo el volumen de participación, sino también su calidad. Pues no sólo la participación de la población depende de la información que reciban sobre el biobanco, sino también la valoración ética y científica de todo el proceso: cuanto mejor informados estén los ciudadanos, más autónoma será su decisión, y más fiable las relaciones que mantengan con los investigadores.

Aunque los aspectos técnicos de una red paneuropea de biobancos son difíciles de aprehender y discutir en un grupo de participantes legos, existen modelos para promover la deliberación pública sobre biobancos que hacen pensar en nuevas posibilidades de gobernanza, pasando del actual modelo de "gobernanza por comités" a otro de "gobernanza participativa" en el que el énfasis en el reparto de beneficios de paso a una mayor atención al reparto de poder en la toma de decisiones. Para ello necesitamos también infraestructuras internacionales con las que abordar las implicaciones éticas, legales y sociales de la investigación genómica que utiliza biobancos. Ya se están dando pasos en esa dirección; el más reciente es el proyecto ELSI 2.0, que pone en marcha una red de coordinación similar en cierto sentido a la BBMRI dedicada a estudiar y armonizar esas implicaciones (Kaye et al. 2012).

REFERENCIAS

Casado da Rocha, A. 2010. Biobancos, cultura científica y ética de la investigación. DILEMATA. International Journal of Applied Ethics 2(4), 1-14.

Gaskell, George et al. 2010. Europeans and Biotechnology in 2010: Winds of change? A report to the European Commission's Directorate-General for Research (Eurobarometer 73.1). Luxembourg: Publications Office of the European Union.

Kaye, Jane et al. 2012. ELSI 2.0 for Genomics and Society. Science 336 (11 May 2012), 673-4.



Hacia el **nuevo** sistema de información social

Las tecnologías de la información y la comunicación (TIC) abrigan una "dualidad": pueden constituir grandes aliados para las personas con discapacidad o en situación de dependencia, pero también pueden provocarles "grandes barreras".

"Lo importante es normalizar los sistemas y diseñarlos para todos, con los mismos estándares". En esta línea, el reto de las nuevas tecnologías "es la atención a la dependencia", lo que es, además, "una gran oportunidad para la innovación y la creación de cosas nuevas".

Debido al escenario impulso generado con la Ley de Dependencia, las CC.AA están ante un momento único para avanzar en la Atención Social mediante la implantación de un **Sistema de Información Social**. Un Sistema de Información Social diferencial basado en la aplicación de las TIC y que no sólo responda a las necesidades básicas de gestión del Sistema de Dependencia.

Desde Informática El Corte Inglés creemos que sólo, un **Sistema que integre la Información al dependiente en un Expediente Social Único** servirá para proporcionar una atención de calidad mediante la prestación de los servicios asociados al mismo (ayuda domiciliaria, teleasistencia, etc.), además de facilitar su coordinación.

Para ello estamos trabajando en el diseño e implantación de un modelo de **Sistema de Información Social** que integre los distintos aspectos de gestión.



al servicio
de la Atención Social

www.ieci.es

INFORMÁTICA

El Corte Inglés

Entrevista

Esther Mitjans Perelló

Directora de la Autoridad Catalana de Protección de Datos[1]

¿Cuál es su visión de la situación actual de la protección de datos en España y en su Comunidad Autónoma?

No resulta sencillo expresar una opinión al respecto que se fundamente en indicadores o datos objetivos suficientemente relevantes, por tanto cualquier visión sobre la situación de la protección de datos estará muy basada en percepciones.

Visto con perspectiva temporal creo que la protección de datos ha ido progresando, seguramente no adecuadamente o no a plena satisfacción de las autoridades de control y en general de los profesionales de la protección de datos, pero ciertamente la situación actual no es la de hace 8 o 10 años, en todo caso sabemos que aún queda mucho camino por recorrer.

Todavía hay una excesiva visión formal del cumplimiento de las obligaciones en materia de protección de datos de carácter personal, creo que los responsables de los tratamientos todavía no son conscientes del valor que una gestión responsable de la protección de datos puede aportar a su actividad, sea pública o privada, y la ciudadanía no es todavía suficientemente consciente del valor que tiene su información personal.

También tengo la sensación de que allí donde existen autoridades de control autonómicas en general hay un mayor nivel de cumplimiento, o como mínimo una mayor presencia del derecho a la protección de datos, y no solo en el sector público, observo que se produce un efecto positivo contagioso también hacía el sector privado.

Desde su punto de vista ¿Cuáles son los principales retos a los que se enfrenta la protección de datos en su Comunidad Autónoma?

Es evidente que la reforma de la legislación sobre protección de datos, con el reglamento Europeo que se está elaborando, va a ser un reto para todos, tendremos que explicar la profundidad de la reforma y el impacto que va a tener sobre todos los agentes relacionados con los tratamientos de datos personales, desde los responsables y encargados de tratamiento, pasando por los profesionales y empresas que se dedican a prestar servicios relacionados con la adecuación y los ciudadanos, ese va a ser nuestro reto a medio plazo.



A corto plazo nuestro principal reto es desarrollar con normalidad y eficacia nuestra actividad del día a día, en un contexto económico que dificulta desarrollar nuestra función de control, para lo que cada vez más necesitamos aplicar economías de escala y buscar el mayor nivel de eficiencia posible.

¿Y específicamente en el sector sanitario?

El sector sanitario en Cataluña está especialmente sensibilizado con el derecho a la protección de

[1] *En el momento de cerrar este número, el Parlamento de Cataluña ha procedido a nombrar nueva Directora de la Autoridad Catalana de Protección de Datos a Dña. M. Àngels Barbarà i Fondevila.*

datos de carácter personal, no solo por la actividad de control que desarrolla la Autoridad Catalana de Protección de Datos, si no porque los centros asistenciales en sus diferentes niveles de prestación y especialidad tienen generalmente bien asumidas las obligaciones que se derivan de la normativa, lo que no obsta que se produzcan incidentes con los datos personales y tengamos que intervenir.
Sinceramente no creo que tengan unos retos especiales, son los que tienen y van a tener el resto de responsables de tratamientos, adecuarse a la reforma Europea y que las dificultades presupuestarias no les impidan cumplir con sus obligaciones en materia de protección de datos de carácter personal.

Siempre escuchamos que España es uno de los países con una regulación de protección de datos más estricta pero ¿Significa esto también que el nivel de cumplimiento es mayor que en otros países?

No necesariamente, no hay datos objetivos que permitan afirmar una cosa u otra, ciertamente el hecho de que exista un régimen sancionador que incluye sanciones económicas ha movido muchas voluntades hacía el cumplimiento, pero también hemos podido observar que eso no implica necesariamente que todo el mundo cumpla.
En otros países de la Unión Europea sin sanciones de ese tipo el nivel general de cumplimiento seguramente es similar, o incluso superior, ya que los responsables de tratamientos tienen mucho más interiorizada la protección de datos como valor añadido a sus actividades, y en consecuencia cumplen por convencimiento y no solo por obligación.

¿Qué opina de las propuesta de la Comisión Europea de un nuevo marco regulador de la protección de datos en Europa? ¿Qué impacto tendrán en el sector sanitario?

Me parece que la reforma era necesaria, movernos con los parámetros de una Directiva del año 1995 con los cambios tecnológicos y de uso social de las TIC hacían necesaria una revisión, que si bien deja intactos los ya conocidos principios de protección de datos estos se adecuan a los nuevos tiempos, especialmente en todo aquello que tiene que ver con Internet y su uso privado y empresarial.
El impacto en el sector sanitario no va a diferir sustancialmente del impacto en otros sectores de actividad, lo que trae la reforma es un cumplimento menos formal y más de gestión, por tanto las organizaciones van a tener que adaptarse a esos requisitos de gestión, y aquí es donde vamos a encontrar los impactos más relevantes.

¿Cuáles son las actuaciones previstas de su autoridad en el sector sanitario para el futuro?

Lo cierto es que las actuaciones que como autoridad de control llevamos a cabo en el sector salud tienen un carácter continuado, por tanto se trata de actuaciones más bien de presente, casi del día a día.
Por definición en la Autoridad Catalana de Protección de Datos las actuaciones preventivas son claves en nuestra institución, y en el caso de tratamientos relacionados con datos de salud, si cabe, aún son más relevantes.
No solo atendemos dudas concretas o consultas de carácter general relacionadas con datos de salud que llegan a nuestro servicio de consultoría por los diferentes canales de comunicación que tenemos abiertos, el hecho de que en nuestro consejo asesor haya un representante del gobierno de la Generalidad de Cataluña relacionado con el ámbito de salud facilita la coordinación tanto en actuaciones más concretas como de carácter general.
Como fruto de esa coordinación hemos sido invitados a participar directamente en la definición de proyectos como, por ejemplo, la historia clínica compartida en Cataluña o el acceso de los ciudadanos a su historia clínica a través de internet, en definitiva el sector salud requiere de una atención y soporte especial, y desde la autoridad se los proporcionamos.

Recientemente asistió al IX Foro de Protección de Datos de Salud de la SEIS ¿Qué opinión le merece esta iniciativa? ¿Considera útil la labor que realiza la SEIS en este ámbito?

Creo que hay consenso entre todas las autoridades de control de que se trata de una iniciativa de gran utilidad, nos permite entrar en contacto directo con el sector sanitario y conocer de primera mano cuales son sus necesidades y dificultades en la materia, lo cual tiene un gran valor, resultando muy eficiente poder reunir en un mismo espacio físico y temporal a tantos profesionales relacionados con el tratamiento de datos de salud.
Tengo la impresión de que también para los profesionales que asisten, tener acceso directo y cercano a las autoridades de control supone un valor añadido de la iniciativa.
Por ello considero de un gran interés la organización por parte de la SEIS de un foro tan especializado en los tratamientos de datos de salud relacionados con el sector sanitario.

Entrevista

Iñaki Pariente de Prada

Director de la Agencia Vasca de Protección de Datos



¿Cuál es su visión de la situación actual de la protección de datos en España y en su Comunidad Autónoma?

La visión que tenemos en la AVPD sobre la protección de datos en Euskadi es positiva, sobre todo a la luz de los resultados del estudio realizado por el Gabinete de Prospección Sociológica, en el que se pone de manifiesto que aumenta la sensibilidad de la población vasca ante la protección de datos personales, al tiempo que se mantiene en niveles muy elevados, hasta el 94%, la confianza en el uso que las administraciones públicas vascas hacen de los datos personales. Y si tenemos en cuenta que nuestro ámbito de actuación son precisamente las administraciones públicas vascas, pienso que el grado de control y de colaboración que mantenemos está dando resultados muy positivos.

Este estudio, que se puede consultar en nuestra página web -avpd.es- nos indica además que el 88% de la población consultada desea más información de la Agencia sobre sus derechos a la protección de datos, lo que nos alienta a continuar impulsando la labor preventiva que venimos realizando.

Desde su punto de vista ¿Cuáles son los principales retos a los que se enfrenta la protección de datos en su Comunidad Autónoma? ¿Y específicamente en el sector sanitario?

Con carácter general, tenemos pendiente un reto importante en todo lo que tiene que ver con Administración Electrónica. En esta época, las administraciones públicas se encuentran en una fase en la que necesitan el intercambio de información como medio de lucha contra el fraude, y para tener un mejor servicio público. Sin embargo, estos intercambios de información no siempre se producen con respeto a la legislación vigente en materia de protección de datos. Debemos mostrarnos vigilantes al respecto e intentamos igualmente reforzar nuestro papel de asesoramiento de las administraciones en aras a una mayor eficacia y respeto del derecho fundamental de los ciudadanos a la protección de sus datos personales.

En el sector sanitario en concreto, hay una cuestión que en los próximos tiempos nos plantea los principales desafíos, cual es la implantación de la historia clínica electrónica única.

La definición de los niveles de seguridad en la protección de estos datos configurados como de especial protección en la LOPD y en su Reglamento de desarrollo, la definición de los accesos a los mismos, o las posibilidades de ejercicio de los derechos de los ciudadanos en relación a este expediente único, son algunos de los retos que se plantean en este sector.

Conviene destacar que la Agencia Vasca de Protección de Datos ha trabajado en el pasado y de forma reiterada en colaboración con el Ente público OSAKIDETZA/SERVICIO VASCO DE SALUD, y es de prever en esta materia una colaboración estrecha en el futuro para eliminar cualquier duda en la materia desde el origen.

Siempre escuchamos que España es uno de los países con una regulación de protección de datos más estricta pero ¿Significa esto también

que el nivel de cumplimiento es mayor que en otros países?

No se si es posible establecer parámetros de comparación con otros países. Desde luego, es una intención clara de esta Agencia Vasca continuar en la gran labor realizada hasta la fecha de información a la ciudadanía, incluso realizando una labor de concienciación en materia del derecho fundamental a la protección de los datos personales.
Lo que si podemos afirmar, porque el Estudio Sociológico realizado así nos lo confirma es que la sociedad vasca tiene gran confianza en el uso que las administraciones vascas hacen de sus datos personales. Y si tenemos en cuenta que los datos que poseen las administraciones están entre los especialmente protegidos, o son muy sensibles, pensemos en los datos de salud, de renta, de seguridad, o educativos, no deja de ser un indicador importante del nivel de cumplimiento.

¿Qué opina de las propuestas de la Comisión Europea de un nuevo marco regulador de la protección de datos en Europa? ¿Qué impacto tendrán en el sector sanitario?

El nuevo Reglamento Europeo en materia de protección de datos tiene algunas características que merece la pena destacar, y que pueden suponer una revolución en el sector.
Por ejemplo, y como ya comentó acertadamente Don Emilio Aced en el número 93 de esta revista , los temas más relevantes son la regulación del principio de minimización de los datos, en conexión con el principio de calidad, la introducción expresa de la mención a los menores en el Reglamento, la mención también expresa al derecho al olvido, derecho que a pesar de estar conceptualmente ya desarrollado se incluye por primera vez en la regulación positiva; la introducción expresa en la norma de los principios "privacy by design" y "privacy by default", en referencia a la introducción de la protección de datos personales ya en el diseño, el primero de ellos, y por defecto en el segundo; muy relevante también, aunque se han establecido ya algunas dudas sobre ello, el incremento del papel del delegado de protección de datos; y por último, y especialmente relevante, el incremento y homologación del papel de las Autoridades de Control, que pasan a tener una consideración mucho más reforzada con esta norma.
Al mismo tiempo que el Reglamento, se está profundizando en materia de protección de datos en el ámbito de la cooperación judicial y policial, de tal manera que hay ya un borrador de Directiva en la materia.
Es especialmente destacable la relevancia que la Comisión Europea y el propio Parlamento Europeo están dedicando a esta materia, como lo indica que el instrumento elegido para la regulación general sea un Reglamento comunitario, que es una norma de obligado cumplimiento para los Estados miembros y los ciudadanos europeos desde su entrada en vigor, sin que sea necesario ningún acto de incorporación al ordenamiento interno del Estado, de forma directa.
Y por último, me gustaría destacar una cuestión que me parece especialmente importante, y que esperamos, como autoridades de control, que permanezca tal y como está en la redacción definitiva, cual es la competencia de las autoridades de control del lugar del domicilio del destinatario del servicio, lo que eliminaría los problemas a los que nos enfrentamos en estos momentos y que se plasman en la cuestión prejudicial planteada por la Audiencia Nacional en relación con la competencia de autoridades y tribunales de los Estados miembros en asuntos relacionados con empresas que tienen su sede en Estados Unidos u otros estados no comunitarios. Con esta redacción, siempre que un ciudadano europeo se ha visto perjudicado en su derecho a la privacidad y a la protección de sus datos personales, incluso en este caso, serían competentes autoridades de control y tribunales de los Estados miembros.
En relación con el ámbito sanitario específicamente, sí que podemos aventurar una mayor protección de los datos sanitarios en el Reglamento, y sobre todo una mayor coordinación y colaboración en el ámbito europeo. Ello resulta obligado para garantizar la continuidad de la asistencia sanitaria transfronteriza, para lo que deben establecerse condiciones armonizadas para el tratamiento de esos datos, sujetas a todas las garantías necesarias.
Las novedades más importantes vinculadas con los datos de salud, que podrían destacarse serían las siguientes:

a) El Reglamento amplía de manera notable el concepto de "los datos relativos a la salud", como categoría de datos que merecen mayor protección, y define, por primera vez, " los datos genéticos" y los " datos biométricos". Los datos genéticos ya gozan en la actualidad de especial protección, dado que el RDLOPD los considera datos relacionados con la salud de las personas,.
b) Interesa también destacar que siendo una de las grandes novedades del Reglamento proyectado

la obligación de evaluar el impacto a la protección de datos de tratamientos que entrañen riesgos específicos para los derechos de las personas, entre las operaciones sujetas a esta evaluación se contemplan aquellas destinadas a analizar su estado de salud, el tratamiento a gran escala de información sobre la salud o destinada a la prestación de atención sanitaria, investigaciones epidemiológicas o estudios relativos a enfermedades mentales o infecciosas, cuando los datos sean tratados con el fin de tomar medidas o decisiones sobre personas concretas , y también el tratamiento de datos genéticos o biométricos .

¿Cuáles son las actuaciones previstas de su autoridad en el sector sanitario para el futuro?

Como ya he dicho anteriormente, y respondiendo a los retos que tenemos encima de la mesa, es especialmente importante la colaboración con la Administración sanitaria en la implantación de la historia clínica electrónica única para que sea respetuosa con la normativa de protección de datos, como desafío y ámbito de actuación inmediato.
Igualmente, es preciso seguir colaborando en todos los aspectos relacionados con el historial clínico En este sentido existe el Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica que regula esta cuestión en el País Vasco,
Asimismo, el ejercicio de los derechos del ciudadano en materia de protección de datos en el ámbito sanitario, sobre todo el acceso a su documentación clínica, en ocasiones plantea algunos problemas, que intentamos resolver conjuntamente.
Probablemente, el terreno donde mayor cuidado hemos de poner es en una de las áreas que en los últimos años más se han intentado desarrollar, como es la atención socio-sanitaria. Este tipo de actuaciones, simultáneas y sinérgicas de los servicios sanitarios y los servicios sociales, actúan sobre colectivos especialmente vulnerables, y se hacen necesarias normalmente en momentos críticos para los ciudadanos beneficiarios, en los cuales la protección de sus intereses vitales puede llevar a minusvalorar las garantías en el tratamiento de sus datos personales. Pero no hemos de olvidar que la habilitación legal para el tratamiento de los datos de salud y la de las atenciones sociales tienen distintas bases legales y debe cuidarse de que esta necesaria y deseable coordinación no lleve a tratamientos indebidos de los datos de los ciudadanos.

Recientemente la AVPD ha participado en el IX Foro de Protección de Datos de Salud de la SEIS ¿Qué opinión le merece esta iniciativa? ¿Considera útil la labor que realiza la SEIS en este ámbito?

En efecto, la AVPD viene colaborando con la SEIS desde el año 2005, año en el que tuvo lugar el II Foro de Protección de Datos de Salud, precisamente en Bilbao. Posteriormente, tras haber suscrito un convenio en el año 2007, hemos participado tanto en el comité de programa, perfilando contenidos y persuadiendo ponentes, como de forma activa, con la participación directa en las mesas y seminarios que se han organizado.
Para nosotros, la colaboración con la SEIS resulta fundamental, porque contribuye a conformar un instrumento de reflexión, debate y difusión, como es el Foro, que viene promovido desde el propio sector, con lo que ello tiene de garantía de aceptación por los que resultan ser, para nosotros, unos aliados esenciales, precisamente por la importancia que tienen los datos de salud como datos especialmente protegidos.
Pienso que se ha conseguido una simbiosis muy positiva, una relación de "gana-gana", porque, por un lado, el sector sanitario tiene a su entera disposición, durante dos días, a las cuatro Autoridades de Control, es decir, los actores principales que en el día a día les van a marcar criterio respecto de la confidencialidad en el tratamiento de sus datos, con sus informes jurídicos, recomendaciones e instrucciones, o que les van a corregir en sus actuaciones, cuando estas no se ajusten a derecho o no se hayan producido con las suficientes garantías de seguridad respecto de los pacientes.
Pero también, por otro, las cuatro Agencias tenemos la ocasión dirigir nuestros mensajes a los mejores expertos en el terreno de la gestión sanitaria, o los responsables de construir los sistemas que han de dar soporte tecnológico a dicha gestión sanitaria, ocasión que procuramos aprovechar para mejorar su conciencia acerca de cómo aplicar, por ejemplo, el principio de "privacidad desde el diseño", minimizando los datos que se solicitan, aplicando las medidas de seguridad de forma integrada o garantizando la trazabilidad de los tratamientos efectuados.
En definitiva, pienso que si no existiese el Foro de Protección de Datos de Salud, tendríamos que inventarlo.

SOLUCIONES TIC INTEGRALES, INTEROPERABLES Y EXTENSIBLES A CUALQUIER ENTORNO SANITARIO



CSC | HEALTHCARE GROUP

Nuestras Soluciones TIC crean un nuevo modelo de cooperación entre todos los profesionales involucrados en el proceso asistencial, incrementando la eficiencia y la calidad de los servicios que prestan a sus pacientes.

Hasta el momento nos ha conocido como iSOFT, uno de los principales proveedores de soluciones de tecnologías de la información para Sanidad. Ahora, desde el 1 abril de 2012, formamos parte del Grupo de Sanidad de CSC, una de las mayores multinacionales proveedoras de soluciones tecnológicas empresariales.

En el centro del Grupo de Sanidad de CSC estaremos respaldados por la magnitud y el compromiso de una compañía mundial que cuenta con más de 98.000 profesionales en 90 países de los cinco continentes, situándonos en un lugar privilegiado para diseñar, desarrollar e implementar las soluciones más innovadoras de la industria, además de incorporar nuevos servicios, enriqueciendo nuestra cartera y mejorando, por tanto, la oferta de valor que ofrecemos al sector salud.

www.csc.com/health_es

Entrevista

Santiago Abascal Conde

Director de la Agencia de Protección de Datos de la Comunidad de Madrid



¿Cuál es su visión de la situación actual de la protección de datos en España y en su Comunidad Autónoma?

Desde el nacimiento de la normativa en materia de protección de datos, en el año 92, han pasado 20 años y entiendo que se ha alcanzado un nivel de conocimiento en la materia lo suficientemente amplio como para pasar de una situación de implantación progresiva a una exigencia más estricta de su cumplimiento.

En este momento ya no puede utilizarse como argumento para el no cumplimiento de determinados preceptos, la dificultad que supone la implantación de los mismos por las características específicas del ámbito sanitario, en especial en el ejercicio de la actividad asistencial. Hemos dispuesto del suficiente período transitorio para adaptar las organizaciones y unidades a las obligaciones impuestas por la normativa de protección de datos.

De hecho, el ciudadano cada vez es más consciente de sus derechos y está ejerciendo las acciones de reclamación cada vez con más asiduidad, y no sólo con el planteamiento de denuncias y tutelas de derechos ante las autoridades de control, sino en los ámbitos civil, mediante la exigencia de responsabilidad patrimonial y las consiguientes indemnizaciones, y en el ámbito penal. En la Comunidad de Madrid, así como en el resto de Comunidades Autónomas que disponen de su específica Autoridad de control, el hecho de disponer de un referente cercano al responsable de los tratamientos de datos que realiza actuaciones de asesoramiento y consultoría ha proporcionado una mayor concienciación y, por consiguiente, un mayor cumplimiento de la normativa de protección de datos.

Desde su punto de vista ¿Cuáles son los principales retos a los que se enfrenta la protección de datos en su Comunidad Autónoma?

Los tratamientos de datos personales están evolucionando a una velocidad sorprendente, empujados por los avances diarios que se producen en el ámbito de las tecnologías de la información y la comunicación. La proliferación de las redes sociales y los nuevos sistemas de disponibilidad de los datos basados en la computación en la nube, por ejemplo, plantean nuevas brechas para la seguridad de la información y, por consiguiente, para el respeto a los derechos de los ciudadanos.

El crecimiento exponencial de la capacidad de gestión y tratamiento de datos personales, al utilizar estas nuevas tecnologías, hacen crecer también de forma exponencial los riesgos y, sobre todo, las consecuencias que pueden tener cualquier tipo de filtración de la información. Las amenazas, que se circunscribían al ámbito espacial en el que se encontraban almacenados los datos y a las ubicaciones concretas en que se realizaban los tratamientos, se han globalizado al igual que los sistemas de almacenamiento y explotación.

La implantación de los nuevos modelos de gestión de la información, no obstante, no deben verse únicamente como una amenaza, sino deben tratar de aprovecharse como una oportunidad de mejora para implantar todas aquellas medidas necesarias para garantizar el respeto a los derechos fundamentales de los ciudadanos y, conseguir esta percepción por los responsables, así como promover medidas concretas para alcanzarlo creo deben ser el objetivo de las actuaciones de las autoridades de control.

Debe preocuparnos especialmente el hecho de que si hemos encontrado innumerables problemas para implantar los mandatos establecidos por la normativa de protección de datos en un marco tecnológico "restringido" geográficamente, no seamos capaces de conseguir las previsiones necesarias para garantizar la seguridad en un marco tecnológico "disperso".

¿Y específicamente en el sector sanitario?

Una de las principales preocupaciones de la APDCM en el ámbito sanitario es tratar de conjugar la globalización de la prestación sanitaria, en la que los pacientes tienen cada vez mayores posibilidades de elección del centro o profesional sanitario en el que ser atendidos, así como posibilitar el acceso y disponibilidad de sus datos sanitarios en cualquier punto en el que tenga que ser atendido por los profesionales sanitarios que intervengan en su asistencia, con el necesario respeto a su intimidad, la confidencialidad de sus datos y facilitarle el ejercicio del derecho de acceso a los mismos.

Las mejoras en la capacidad de gestión, tan necesarias en estos momentos, no deben hacerse sacrificando los derechos individuales de los ciudadanos. La eficacia y la eficiencia de los servicios sanitarios deben tener como referente, siempre, el respeto más absoluto de la intimidad y confidencialidad de los datos personales.

Siempre escuchamos que España es uno de los países con una regulación de protección de datos más estricta pero ¿Significa esto también que el nivel de cumplimiento es mayor que en otros países?

La idea de que el marco de regulación de la protección de datos en España era más riguroso que en otros países de la Unión Europea se ha generado por la imposición de determinadas obligaciones formales de la normativa española, así como por la cuantía de las sanciones económicas que establece su régimen sancionador.

Las obligaciones formales han constituido una importante vía para conseguir una inicial toma de contacto de los responsables de los tratamientos de datos con la normativa de protección de datos, promoviendo un mejor cumplimiento del resto de las obligaciones impuestas por la misma. El régimen sancionador, por su parte, ha sido objeto de importantes atenuaciones, permitiéndose inicialmente aplicar sanciones de menor cuantía, así como con la implantación de la figura del apercibimiento como medida para evitar la imputación de sanciones iniciales.

Atendiendo al marco general establecido por la Directiva Europea 96/46/CE, no creo que existan diferencias sustanciales en cuanto al nivel de cumplimiento del marco normativo general de la protección de datos en los diferentes países de nuestro entorno. Las diferencias pueden encontrarse en las particularidades propias de la normativa de trasposición de cada uno de los Estados.

¿Qué opina de las propuestas de la Comisión Europea de un nuevo marco regulador de la protección de datos en Europa? ¿Qué impacto tendrán en el sector sanitario?

Parece adecuado que la Comisión se plantee homogeneizar la regulación de protección de datos en todos los países de la Unión, evitando las diferencias generadas por las normas estatales de trasposición de la Directiva 95/46/CE. Lo que hará más efectivo el derecho de circulación de personas y datos dentro del ámbito territorial europeo.

Del análisis del proyecto de Reglamento que se encuentra en tramitación podemos obtener dos claras conclusiones; aún cuando se propone eliminar determinadas obligaciones formales como por ejemplo, la inscripción de los ficheros o tratamientos de datos en los registros de las autoridades de control, se cran nuevas obligaciones de generación y conservación de documentación que van a suponer una importante carga formal para los responsables; el nuevo régimen sancionador que se propone, no diferencia entre tratamientos de datos de titularidad pública o privada y el marco de las cuantías de las sanciones es bastante elevado.

En concreto, para el ámbito sanitario, al ampliarse el concepto de dato relacionado con la salud y seguir siendo considerado éste como especialmente protegido, va a suponer para las instituciones y organizaciones sanitarias la necesidad de realizar más actuaciones para garantizar los tratamientos de datos conforme al nuevo marco regulatorio que se establece.

¿Cuáles son las actuaciones previstas de su autoridad en el sector sanitario para el futuro?

Partiendo de las solicitudes y consultas que revimos en la Agencia de los ciudadanos y responsables de los tratamientos, así como vistas las sentencias que están emanando de los diferentes ámbitos jurisdiccionales, creo que las actuaciones más relevantes que debemos llevar a cabo son:

- Mejorar los sistemas de control de acceso por parte de los profesionales sanitarios a la documentación clínica de los pacientes, consiguiendo limitarla de una forma efectiva a aquellos que tengan una relación directa con la atención sanitaria al paciente.

- Mejorar los tratamientos de datos de salud que no forman parte de la actividad asistencial: docencia, investigación, gestión de los centros, etc. Garantizando el respeto a los derechos que la normativa establece y conseguir un cumplimiento riguroso de las obligaciones impuestas por la normativa.
- Facilitar el ejercicio de los derechos de acceso, rectificación y cancelación de datos por parte de los pacientes y usuarios de las instituciones sanitarias públicas de la Comunidad de Madrid.

Atendiendo al nuevo marco normativo que propone el proyecto de Reglamento de la Comisión Europea, debemos empezar a trabajar como implantar el "derecho al olvido" en el ámbito sanitario, así como regular y normalizar los procedimientos y plazos de conservación de la documentación clínica.

Recientemente asistió al IX Foro de Protección de Datos de Salud de la SEIS ¿Qué opinión le merece esta iniciativa? ¿Considera útil la labor que realiza la SEIS en este ámbito?

El Foro de Protección de Datos que viene organizando la SEIS todos los años en Pamplona constituye un importante punto de encuentro para los profesionales del sector sanitario, en el que analizar diferentes aspectos de la actividad sanitaria desde el punto de vista del cumplimiento de la normativa de protección de datos. Es el único evento en España en el que participan conjuntamente todas las autoridades de control en materia de protección de datos, lo que le dota de una especial relevancia en la materia.

Todas las Agencias de Protección de Datos se han implicado a lo largo de estos años en su organización y tienen una importante participación en el mismo, permitiéndoles captar las dudas que se plantean los profesionales sanitarios en su día a día, así como difundir los criterios que vienen aplicando en la resolución de los asuntos que se les presentan en el ejercicio de sus actuaciones.

El eminente planteamiento práctico de las sesiones que componen el Foro le dota de una especial utilidad para los responsables y gestores de los centros e instituciones sanitarias, permitiéndoles afrontar con mayor seguridad el ejercicio de su actividad.



I SEMINARIO DE PROTECCIÓN DE DATOS EN LA ATENCIÓN SOCIOSANITARIA

INAUGURACIÓN

Con carácter previo al IX Foro de Datos de la Salud, se celebró el "Seminario sobre Protección de Datos en la Atención Sociosanitaria", que fue impartido por miembros de la Agencias de Protección de Datos. La inauguración del seminario corrió a cargo de Doña Elena Torres Miranda, consejera de Política Social, Igualdad, Deporte y Juventud del Gobierno de Navarra, que además de agradecer la existencia del Foro de Datos de la Salud, hizo referencia a la obligación que tienen todas las Administraciones públicas, que manejan un gran volumen de datos sensibles, de cumplir con la LOPD. Además, este cumplimiento supone la prestación de una mayor calidad del servicio público. También incidió en que no puede haber un uso abusivo de los datos personales y que se debe incidir en la formación del personal.- "Hay que crear una conciencia colectiva sobre el manejo de la información sensible".

"SEMINARIO SOBRE PROTECCIÓN DE DATOS EN LA ATENCIÓN SOCIOSANITARIA"

María José Blanco Antón,
Secretaria General AEPD

Su exposición estuvo enfocada a dar una visión general de la normativa vigente de protección de datos, incluyendo también la tramitación que se está llevando a cabo en la actualidad para aprobar lo que será el Reglamento de Protección de Datos de la Unión Europea. Asimismo, también citó los principios de protección de datos y las obligaciones del responsable del fichero.

Sobre estas obligaciones, destaca en el ámbito público el procedimiento para la elaboración de los ficheros, que deben ser comunicados a la AEPD utilizando el sistema NOTA. Además, la AEPD ha puesto a disposición de los responsables una nueva herramienta –DISPONE- que sirve de apoyo para la elaboración de esas disposiciones.

Por otra parte, también hizo referencia a la existencia de los Códigos Tipos, que son un sistema de auto-regulación, siendo obligatorios para todos aquellos que se adhieran. Puso como ejemplo el Código Tipo de ACRA (Asociación Catalana de Recursos Asistenciales), haciendo referencia a su contenido. Así, según este Código se deberá solicitar el consentimiento expreso y escrito para los datos de religión de los pacientes que se refieran a la asistencia a ritos religiosos, alimentación o transfusiones de sangre.

Por otra parte, también analizó un supuesto práctico.- el Libro de socios de entidades de juventud. Respecto a este Libro, que es un fichero de datos de carácter personal, es posible que se traten datos de religión o creencias por lo que será necesario consentimiento expreso, y las medidas de seguridad de nivel alto.



Emilio Aced y Mª José Blanco

Jordi Ferreres i Jovani
Secretario General ACPD.

Le correspondió explicar con detalle los principios en que se fundamenta la protección de datos de carácter personal y que están regulados en la LOPD y en su Reglamento de desarrollo.

En este sentido, desglosó el principio de calidad de datos personales, el derecho de información, el principio del consentimiento, el deber de secreto, el ré-

gimen jurídico de las cesiones de datos de carácter personal, así como el estatus del encargado del tratamiento. También hizo referencia a una serie de casos prácticos como las solicitudes de subvenciones, que debe aplicarse la normativa de protección de datos personales, sobretodo el principio de calidad de datos para no solicitar más documentación que la necesaria; la difusión de datos personales, siendo necesario el consentimiento o habilitación legal, además de aplicar el principio de proporcionalidad, e implementar las medidas de seguridad necesarias; y la relación entre los servicios sanitarios y los sociales sobre el intercambio de información, de manera que si se realiza entre la Administración una Comunidad Autónoma y un Ayuntamiento tendrá la consideración de cesión de datos de carácter personal.

Ángel Igualada Menor
Subd. General Adjunto Registro de Ficheros y Sistemas de Información. APDCM.

Su ponencia estuvo enfocada a la explicación de los derechos de protección de datos.- acceso, cancelación, oposición y rectificación. Estos derechos forman parte del contenido del derecho fundamental a la protección de datos y facilitan que el ciudadano tenga el control de sus datos.

Respecto al derecho de acceso, si bien es diferente al que recoge la Ley 30/1992 o la Ley 41/2002, su contenido es similar. Su ejercicio deber realizarse ante el responsable y éste tiene la obligación de responder, incluso aunque el ciudadano no haya utilizado el formulario habilitado por el citado responsable para ejercitar dicho derecho.

En cuanto al derecho de oposición, es ejercitable, por ejemplo, ante los ficheros de publicidad y prospección comercial. Ligado a este derecho, existe también la impugnación de valoraciones (cuando se realiza la valoración de una persona basada en su rendimiento laboral, solvencia económica o la propia conducta del sujeto). Asimismo, el procedimiento para ejercitar estos derechos es similar al del ejercicio del derecho de acceso.

Respecto a los derechos de rectificación y cancelación, respecto al primero, se puede solicitar al responsable la modificación de cualquier dato que sea incorrecto, acreditando la citada incorrección, y respecto al segundo, la supresión de aquellos datos que sean inadecuados o excesivos.

Termina comentando un supuesto práctico relativo al conocimiento por parte de un denunciado de la persona que ha realizado la denuncia. Si se accede, de acuerdo a la Ley 30/1992, al expediente administrativo por el denunciado se podría conocer. También estaría justificado aplicando el derecho fundamental a la tutela judicial efectiva. El criterio de la APDCM es que se facilite, salvo que exista un interés mayor para salvaguardar el nombre y apellidos de la persona que ha realizado la denuncia.

Pedro Alberto González González
Responsable del Registro de Ficheros y Nuevas Tecnologías. Agencia Vasca.

Comenzó su presentación haciendo una distinción entre las medidas de seguridad organizativas y técnicas, poniendo énfasis en que quizás, las primeras sean más importantes, y citando diversas normas legales del País Vasco que han recogido en algunos de sus artículos menciones sobre protección de datos, como puede ser la Ley 12/2008, de servicios sociales de esa Comunidad, y su artículo 9 que se refiere al consentimiento en el ámbito de esa servicio público.

Por otra parte, expuso que la finalidad de la seguridad es evitar riesgos, y que la misma debe ser incluida en la elaboración de las herramientas informáticas. Puso como ejemplo la "Privacidad por diseño".

Asimismo, desglosó las medidas de seguridad en relación con los tres niveles de seguridad existentes en función de la categoría de datos personales recabados.- bajas, medias y altas, incidiendo sobre todo, en la existencia de una política dentro de la organización respecto al uso de equipos portátiles y "pendrives", y la política de "escritorio de trabajo limpio".

Por último y como conclusión del seminario, los asistentes plantearon diversas cuestiones a los ponentes referentes al objetivo final que se busca con la implantación de las medidas de seguridad, el tratamiento de datos de salud por parte del personal de los servicios sociales y la relación que se puede entablar entre un paciente y un médico utilizando una red social teniendo en cuenta su implicación desde el punto de vista de protección de datos.



Pedro Alberto Gonzalez

IX FORO SOBRE PROTECCIÓN DE DATOS



ACTO INAUGURAL

Luciano Saéz Ayerra, presidente de la SEIS, comenzó dando la bienvenida agradeciendo la colaboración al Gobierno de Navarra, su Consejería de Salud, a la Sociedad de Desarrollo de Navarra y a las Agencias de Protección de Datos.

Destacó que una de las misiones de la SEIS es la formación en materia de protección de datos, y que debe existir un canal para que los profesionales sanitarios en tecnologías puedan transmitir a la Agencias sus dudas e inquietudes sobre la aplicación de la normativa de protección de datos. Asimismo, hizo un breve repaso de los objetivos del IX Foro sobre Protección de Datos y de los temas que se van a tratar en cada una de las sesiones que forman parte del citado IX Foro.

Por su parte, **Carlos Fernández Valdivieso**, director Gerente de SODENA, recalcó la importancia de la implantación de la protección de datos personales para salvaguardar los datos de salud, que tienen la consideración de especialmente protegido y que la atención sanitaria del Siglo XXI se basa en poner la información al servicio de la misma.



Marta Vera Janín, consejera de Salud del Gobierno Vasco, se refirió a que tanto la historia clínica informatizada como los ficheros centralizados generan cierta inquietud, sobre todo a nivel técnico.
En este sentido, las organizaciones sanitarias deben dar respuesta a estas inquietudes, aplicando las medidas de seguridad adecuadas para garantizar los datos personales, independientemente desde donde se accede a los mencionados ficheros. Además, la seguridad comienza con una buena organización de las entidades, en este caso, de los centros hospitalarios. Pero junto con la adopción de las medidas de seguridad correspondiente, debe haber un compromiso por parte de los profesionales

CONFERENCIA DE D. JOSÉ LUÍS RODRÍGUEZ ÁLVAREZ, DIRECTOR AEPD

Comenzó haciendo hincapié en el régimen jurídico específico de los datos de salud.- existencia de consentimiento expreso, infracciones muy graves en caso de incumplimiento y adopción de medidas de seguridad de nivel alto.
También se refirió a la evolución jurídica entre la normativa de protección de datos y la que regula la sanidad de forma específica, ya que existe una interrelación entre ambos bloques normativos. Así, la primera establece una serie de principios, mientras que la segunda garantías a los pacientes.
Además, en ocasiones la normativa sanitaria ha ampliado la información que debe recibir un paciente, por ejemplo, en materia de investigación biomédica, o la regulación del acceso a la historia clínica. Otro valor a destacar, que comparten ambas regulaciones, es la confidencialidad.
Por otra parte, y en referencia a los biobancos, realizó una crítica a la definición que aparece en el Reglamento de Biobancos sobre quién es responsable del fichero. A su juicio, la postura sigue siendo la misma que ya manifestó la AEPD cuando se elaboró el citado Reglamento.- el responsable será quien decida sobre el uso y finalidad de los datos.
En cuanto a las posibles transferencias internacionales de datos genéticos, hay que estar a la regulación vigente, sobre todo en lo referente a las autorizaciones cuando se transfieren este tipo de datos a países que no tiene reconocido el nivel de adecuación.
Por otra parte, hizo un repaso de las actuaciones de la AEPD en el ámbito sanitario, entre ellas, el Plan de Inspección iniciado en el año 2010 sobre la situación de cumplimiento de la LOPD en hospitales públicos y privados. Este Plan vino motivado por las numerosas noticias en prensa.- aparición de historiales en la basura, filtración de historias clínicas usando redes P2P, etc.
De los resultados del informe elaborado en el marco de ese Plan de Inspección destacó dos aspectos.- tanto en el registro de accesos como en la auditoria bianual se mostró un elevado incumplimiento, sobre todo en los de carácter público. Aunque tras el informe, numerosos hospitales empezaron a realizar el cumplimiento de la LOPD desde el punto de vista formal, especialmente en lo que se refiere al registro de fichero, todavía existen numerosas deficiencias al respecto.
También comentó algún expediente sancionador, como el caso de la publicación en una página web de datos de salud de un paciente, aunque se había realizado con fines de investigación. El problema es que la información estaba accesible a cualquiera introduciendo el nombre y apellidos de la persona a través de un buscador.
Por último, analizó los problemas surgidos del "cloud computing". Si bien tiene efectos favorables en materia de gestión y ahorro económico, las Autoridades de Control se plantean cuál es la legislación aplicable –al poder existir varios territorios-, como se configura la relación jurídica entre el proveedor y los clientes, cuáles son las medidas de seguridad, y como se respeta el régimen de transferencias internacionales.
También anuncia que el Grupo del Artículo 29 está trabajando en un Dictamen sobre "cloud computing" que será aprobado seguramente en junio de este año, y citando que la AEPD abrió un período de información pública, habiendo recibido numerosas propuestas y opiniones sobre este tema. Además, en el ámbito de la salud, los servicios de "cloud computing" deberán ser más diligentes.
Termina refiriéndose a las conclusiones iniciales de la AEPD sobre "cloud computing".-

- El responsable que contrate el "cloud" no pierde de tal condición, debiendo cumplir con la LOPD, sobre todo lo referente a las transferencias internacionales.
- La empresa que suministre el "cloud" es un encargado del tratamiento.
- La ley aplicable será la del responsable del tratamiento, es decir, quién contrate. En España, será la LOPD. No caben pactos para modificar la ley aplicable, ya que hay algunos proveedo-

res que dan a entender que se puede pactar. La ley aplicable no es "pactable".
- A la hora de contratar, el responsable debe asegurar que el prestador del "cloud" le asegure que cumplirá con la normativa vigente española en lo referente al art.12 LOPD. El contenido de este precepto debe incluirse en el contrato que firmen ambas partes.
- Si la contratación del "cloud" se hace en el ámbito de los servicios de salud de las Administraciones públicos, la Disposición Adicional 26 del Texto Refundido de la Ley de Contratos de las AAPP exige garantías equivalentes, y el tipo de contratos sería el de servicios. Es aconsejable también que las Administraciones designen un responsable del seguimiento del contrato, que podría ser un precedente de la figura del DPO (responsable de protección de datos).
- La intervención de posibles subcontratistas no debe suponer óbice para que también cumplan la LOPD.

PRIMERA SESIÓN: La protección de datos en el día a día de un Gerente de Hospital, ¿Misión Imposible?



Introdujo la sesión **María José Blanco (MJB)**, secretaria General de la AEPD, mencionando que no es una misión imposible, pero sí compleja. También hizo alusión a los resultados del informe de cumplimiento de la LOPD en hospitales, al cual ya hizo referencia anteriormente del Director de la AEPD. El citado informe provocó un mayor cumplimiento de la normativa de protección de datos en los hospitales.

Por su parte, en su papel de moderador, **Javier Carnicero**, del Servicio de Prestaciones y Conciertos, del Servicio Navarro de Salud, preguntó a los miembros de la sesión las siguientes cuestiones.

Pregunta 1: ¿Es misión imposible?

Rosario Cabezudo Vallés (RCV), del Hospital Clínico Zaragoza, manifestó que sí, sobre todo en los hospitales grandes. Existe una gran dificultad.

Juan Antonio Zumalacárregui Villaso (JAZV). Hospital de Cruces. También considera que dado el gran número de pacientes, es bastante complicado. No obstante, en el día a día, cree que se cumple bastante bien. Si vas a una protección de datos estricta, es imposible.

Emilio Aced Félez (EAF). Subdirector de Consultoría y Registro de Ficheros de la APDCM. Reconoce que el entorno es complejo y que hay situaciones críticas. No cree que sea imposible y que, sobre todo, hay que formar al personal y establecer procedimientos claros así como explicar las responsabilidades en que se incurre por no cumplirlos.

Pregunta 2: La normativa sanitaria y la protección de datos se "llevan bien". ¿Es cierto?

RCV. Puso de manifiesto que hay restricciones como el acceso por parte de los familiares. Así, en la de Autonomía pueden tener acceso y por la LOPD podría restringirlo. También cree que difiere mucho si la historia clínica está en papel o está informatizada. La primera lleva un procedimiento para el acceso. En la segunda, la gente suele pasarse las contraseñas.

JAZV.- Recomienda que exista un figura encargada del cumplimiento de la normativa de protección de datos y que trate de resolver los problemas cuando choque la normativa sanitaria con la de protección de datos.

EAF.- En materia de cancelación, hay que estar a lo que regula la Ley de Autonomía del Paciente. La protección de datos no existe para dificultad la asistencia sanitaria sino para garantizar derechos de los pacientes y aportar calidad a la asistencia. En concreto, es impensable que sólo un médico acceda al historial clínico y la protección de datos no impide que hagan uso de él los profesionales que tengan razones para ello.

MJB.- La legislación sectorial sanitaria complementa la normativa de la protección de datos, y en muchos casos, como en la cancelación, la aclara. Sobre lo de comunicarse la claves de accesos, hay que formar al personal para que este tipo de situaciones no ocurra. Comenta también que en materia de prevención de riesgos, la empresa debe conocer si el trabajador es apto o no, pero ninguna información más. Lo pone como ejemplo de cambio, ya que anteriormente, si se conocía la información de salud de los trabajadores.

Pregunta 3: ¿Cómo se ha resuelto tanto en la historia en papel cómo en la electrónica el asunto de las anotaciones subjetivas de los médicos?

RCV.- Tienen establecido un protocolo sobre qué información se da cuando se ejercita el acceso a la historia clínica. En este sentido, no se les da órdenes de tratamiento ni enfermería ni el estado evolutivo del paciente. La mayoría de los accesos vienen motivados por el hecho de cambio de domicilio. Si se trata de un expediente de responsabilidad patrimonial, se une toda la historia clínica al citado expediente. Hay que respetar las anotaciones subjetivas de los médicos, sino las historias clínicas se quedan empobrecidas. El propio médico ya tiene cuidado al escribir dichas anotaciones. Además, deben cumplir el Código Deontológico. Lo que no se puede permitir son anotaciones gratuitas.

JAZV.- También tienen un sistema parecido. Hace hincapié en que es importante conocer el motivo para el que el paciente solicita la historia clínica ya que ello ayuda mucho a la hora de entregarle la documentación adecuada.

EAF.- Considera muy importante la existencia de protocolos para dar la información como, por ejemplo, el expuesto del Hospital de Cruces. Hace hincapié en que en relación con las anotaciones subjetivas, la Ley de Autonomía del Paciente no dice que el paciente no tenga derecho a acceder a ellas sino que el profesional sanitario puede oponerse a dicho acceso. Si no existe dicha oposición, no hay ningún problema en entregarlas.

En la ronda de preguntas, una de las cuestiones que más discusión suscitó fue lo relativo a qué es una anotación subjetiva y como deben de tratarse.

SEGUNDA SESIÓN: Cloud computing en sanidad: situación e implicaciones para la privacidad



Esther Mitjans Perelló (EMP), directora ACPD, como punto de partida, puso de manifiesto que el "cloud computing" se está imponiendo ya que supone una reducción de costes en el uso de las TIC, e incluso cambiará nuestra economía. Así, a modo de ejemplo, puso de relevancia la importancia que tie-

ne en la actualidad en el Reino Unido internet, que es el país donde existe una mayor compra on-line, y cuyos ciudadanos dejarían la mayoría de "hobbies" a favor de internet.
No obstante lo anterior, en las consultas públicas realizadas por la Comisión Europea, CNIL (Autoridad Francesa de Protección de Datos) y AEPD se ha puesto de manifiesto que los ciudadanos desean que exista una protección de la privacidad.
En este sentido, en el documento de la Comisión "Un enfoque global de la protección de datos", se puso de manifiesto la existencia de nuevo retos en materia de privacidad. Entre ellos, los servicios de "cloud". Asimismo, el Grupo de Berlín está trabajando en un documento sobre este tipo de servicios y sus implicaciones en materia de protección de datos. El citado Grupo parte de la base que en materia de sanidad, si no se cumplen una serie de principios garantistas, no deben utilizarse dichos servicios. Entre estas medidas, se encuentran, por ejemplo, la legislación aplicable, la posibilidad de ejercer los derechos ARCO, análisis de riesgos y la realización de auditorías.
Concluye que en la "computación en nube" debe haber la necesaria transparencia en materia de privacidad.

El moderador, **Ramón Miralles (RM)**, coordinador de Auditoría y Seguridad de Información. ACPD, tras introducir a los ponentes, realizó las siguientes preguntas a los miembros de la sesión:

Pregunta 1. ¿Es necesario o imprescindible el "cloud computing"?

Nathaly Rey Arenas (NRA), directora General ISMS Forum-CSA-ES, dijo que lo sería con matices, si queremos dar una buena prestación de servicios, que en este caso, serían los servicios sanitarios. Además significa compartir información, celeridad y evolución tecnológica. Asimismo, los costes irán en función de los recursos utilizados, sin necesidad de tener que crear plataformas de software, de forma, que el ahorro económico al usar el "cloud" se podrá invertir, por ejemplo, en recursos humanos. No obstante, habrá una serie de límites, entre ellos, el respeto a los derechos fundamentales a la protección de datos de carácter personal, intimidad y honor.



Esther Mitjans

Miguel Ángel Máñez Ortiz (MAM), subdirector Económico y de RRHH del Hospital Universitario de Sant Joan dijo que el "cloud" es compartir datos en Internet, existiendo dos tipos de nubes: la reglada u "oficial" que se utiliza para ese intercambio de datos, y la de carácter espontáneo, citando en este caso la existencia de algún servicio "cloud" en el que los pacientes "cuelgan" sus patologías o aquellas que crean los profesionales cuyas demandas no son satisfechas por los servicios TIC de sus organismos.
Hay que preguntar ¿De quién son los datos en el "cloud"? Pone como ejemplo, si a las pruebas de laboratorio podrían acceder los pacientes directamente, ya que de ser así, accederían antes que los hospitales. Considera que el titular de los datos es el paciente.

Albert Arnó Palau (AAP), director General Onmedic Networks, consideró que "es el nuevo internet", ha llegado para quedarse y es una nueva forma de trabajar que ayuda a colaborar en equipo. Permite trabajar directamente en un documento "on-line" a varios usuarios colaborando realmente. Además, hay que reclamar un "derecho a trabajar digitalmente", de manera que cada uno pueda guardar su información en la "nube" y decida quién puede acceder a esa información. Opina que quién no esté trabajando usando el "cloud" será un analfabeto digital.

Pregunta 2. Desde el punto de vista de la protección de datos ¿Dónde existe más riesgo para los datos de salud? ¿En el entorno "cloud" o en los tradicionales como el local o centro de proceso de datos?

NRA.- Depende: habrá más riesgos donde no haya "gobierno de la seguridad". Existen obligaciones que son iguales en ambos tipos ("cloud"/tradicional) como el consentimiento o calidad, pero otros, como el régimen de las transferencias internacionales serán diferentes por la posibilidad de mover los datos de un lugar a otro. Considera que habrá

que valorar los riesgos de seguridad antes de "saltar" al "cloud computing".
En comparativa con una red social, en ésta es el usuario el que controla la privacidad decidiendo qué es lo que "sube"; en el "cloud" se requiere consentimiento expreso al ser datos de salud y tanto el responsable como el prestador de servicio tienen una serie de obligaciones en materia de protección de datos, no teniendo el ciudadano el control para decidir lo que quiere "subir" a la nube.
MAM.- Para responder a esta cuestión hizo un símil preguntando a los asistentes si existen protocolos en los hospitales para seguridad y envío de fax, y seguridad en los carros que se utilizan para distribuir las historias clínicas en papel. Al ser la respuesta negativa, estima que el "cloud" es más seguro.
AAP.- Se fía más de la seguridad de los servicios de la nube que del sistema local.
RM.- Opinó que si bien está de acuerdo en muchas de las opiniones de los intervinientes en la mesa, plantea que diversos estudios han mostrado que existe preocupación por la seguridad de los datos.
En el turno de preguntas, se planteó que algunas empresas en los contratos no cumplen con el artículo 12 de la LOPD referente al encargado del tratamiento.

TERCERA SESIÓN: Casos prácticos: la experiencia de las autoridades de las Agencias de Protección de Datos



El moderador, **Carlos García Codina**, jefe del Área Informática de la Subdirección General TIC del Ministerio de Economía y Competitividad, introdujo la sesión explicando que el objetivo de esta mesa es conocer la doctrina de las Autoridades de Control sobre supuestos prácticos de tratamiento de datos personales de salud. Asimismo, cada representante de su respectiva Autoridad de Control presentará sus casos prácticos.

Julián Prieto Hergueta, subdirector del Registro de Protección de Datos de la AEPD, expuso cuatro casos prácticos seleccionados por la Subdirección de Inspección de la AEPD. El primero relativo al extravío y pérdida de historias clínicas de un Hospital público. El denunciante se dirigió al hospital que le contestó que si en un determinado plazo no se encontrase su historia clínica, se reconstruiría la misma. La historia tardó en recuperarse 5 meses, si bien siguió acudiendo a ese Hospital para recibir la prestación sanitaria correspondiente, en ocasiones no se le pudo atender al haber perdido la historia clínica. La AEPD, valorando todos los hechos, consideró que no se habían adoptado las medidas de seguridad correspondiente, habiéndose infringido el artículo 9 de la LOPD.
El segundo versó sobre la realización de pruebas médicas de un trabajador, antes de incorporarse a una empresa, sin su consentimiento. El centro médico argumentó que había actuado por encargo por la empresa, pero la AEPD consideró que era responsable por haber tratado datos de salud sin consentimiento. Asimismo, se constató que la historia clínica no se custodiaba debidamente. Se habían cometido dos infracciones: tratar datos de salud sin consentimiento y no cumplir con las medidas de seguridad, infracción muy grave rebajada en la escala inferior de acuerdo a la LES (40.000 euros) e infracción grave (40.000 euros).
Respecto al tercero, la denuncia vino motivada porque un particular al introducir su nombre y apelli-

dos en un buscador aparecía en una página web de un hospital con sus datos personales incluyendo cuándo se había realizado las pruebas médicas y el diagnóstico (enfisema). El centro de salud privado reconoció que fue un error ya que la disociación no se había producido correctamente. Para la AEPD se había infringido, además de las medidas seguridad, la vulneración del deber de secreto. Al haber concurso medial, la AEPD impuso la sanción por incumplimiento de las medidas de seguridad.
El último de los supuestos prácticos, los hechos que motivaron el inicio del expediente sancionador fueron el acceso al sistema farmacéutico de una farmacia usando los datos del titular de la misma estando el mismo ausente. Se accedía por el personal de la farmacia, por lo que la AEPD consideró también que se habían vulnerado las medidas de seguridad. No obstante, se aplicó la figura del apercibimiento.

Emilio del Val Puerto, subdirector General de Inspección y Tutela de derechos de la APDCM, trotó un primer supuesto sobre el acceso a la historia clínica por padres separados. Mientras la patria potestad esté compartida podrán acceder ambos. Este tipo de acceso no se considera cesión, sino acceso por medio de representante. Lo controvertido de este acceso es que el mismo se utiliza no para conocer la salud del menor, sino los datos personales del otro progenitor. En la APDCM, se interpuso una denuncia en la que un padre quería conocer toda la vida de su ex-mujer mediante el acceso a la historia clínica. Hubo que hacer un balance entre los derechos del menor y la posibilidad de que la intimidad de la ex-mujer se viese menoscabada, aplicando el principio de proporcionalidad y calidad, de manera que se facilitase los accesos minorando la información de la ex-mujer.



Juana María Vegas Fernández y Emilio del Val Puerto,

El siguiente caso práctico analizado fue sobre las adaptaciones curriculares de los alumnos. Para dichas adaptaciones, con datos de salud, debe existir consentimiento expreso. En este supuesto, se había filtrado información pero no se pudo comprobar de dónde había procedido la fuga de la citada información, por lo que se decidió el archivo de actuaciones.
El tercero, no fue un supuesto de inspección, sino un informe sobre el tratamiento de datos en clínicas forenses. Se resolvió que de acuerdo al Real Decreto 1720/2007 (Reglamento de desarrollo de la LOPD) los datos de los fallecidos están fuera de la LOPD, sin perjuicio de la comunicación del óbito por parte de los familiares.
El último supuesto, se analizó el uso de la historia clínica en los procedimientos de responsabilidad patrimonial, en el que a existir habilitación legal, se puede solicitar copia de la misma para la tramitación de ese procedimiento.

Carles San José i Amat, jefe del Área de Inspección. ACPD, analizó en primer lugar una pérdida de la historia clínica en la que el hospital alegaba que la ACPD tenía que probar que efectivamente se había perdido. Este supuesto estaba relacionado con un derecho de acceso a la historia clínica perdida. La ACPD estimó la tutela de derechos obligando al hospital a reconstruir la historia clínica. Además, se abrió un expediente de inspección por vulnerar las medidas de seguridad, declarando la infracción correspondiente que había cometido el hospital.
En cuanto al segundo de los casos, un ciudadano que ejerció el derecho de rectificación de una anotación a un informe médico en la que se decía "el paciente se va con todo amenazante". La primera respuesta del hospital al paciente fue "la aplicación informática no permite borrar dicho comentario". En el procedimiento instruido por la ACPD, el hospital mantuvo que el ciudadano efectivamente se fue de tal forma. Para la ACPD se trataba de una apreciación subjetiva que no es lo mismo que una anotación subjetiva, ya que esta última incide en el tratamiento médico del paciente. Para la ACPD, posiblemente el dato no fuese inexacto, pero no era necesario para garantizar el proceso asistencial, por lo que en vez de estimar el derecho de rectificación, se estimó el de cancelación.
El siguiente versó sobre un hospital que tenía pacientes de un centro penitenciario que había aprobado un protocolo para dar información a sus familiares. Se denunció que el citado proto-

colo vulneraba las medidas de seguridad. Según este documento, el recluso daba los datos de la persona a la cuál consideraba que se le podía dar su información, es decir, existía consentimiento expreso. El problema era identificar por vía telefónica que realmente era la persona que había sido elegida por el recluso para facilitar la información.

Juana María Vegas Fernández, inspectora y Letrada de la Asesoría Jurídica, AVPD, puso de manifiesto en primer lugar, que durante el año 2011 ha habido una disminución de las denuncias en materia sanitaria, debido a la labor preventiva que está realizando la AVPD. No obstante, sí hay un incremento tanto en reclamaciones de acceso a la historia clínica como de cancelaciones de anotaciones subjetivas.

Centró su participación sobre el derecho de acceso y las anotaciones subjetivas. Así, respecto al primero, la ley 41/2002 lo configura como un derecho del paciente. El resto de accesos, por ejemplo investigadores o jueces, se considera un uso. ¿Tiene que alegar el paciente un interés legítimo para acceder a su historia clínica? Si bien la Ley Vasca de asistencia sanitaria se remite a la Ley 41/2002, la AVPD considera que no tiene que mostrar un interés legítimo.

Por otra parte, también se plantea si se debe acceder a todo o parte de la historia clínica. A su juicio, parece que tanto la Ley 41/2002 como la Ley Vasca de Asistencia Sanitaria, se tiene derecho a la copia de los documentos. Desde una sentencia del TSJ del País Vasco anterior a la ley 41/2002, para la AVPD el paciente tiene derecho al acceso a todo el contenido de la historia clínica, incluyendo las hojas de evolución.

Otra cuestión que puede surgir son los límites en la solicitud de copia en el derecho de acceso, de manera que esos límites, al tratarse de un derecho fundamental, debe ser interpretado de forma estricta. No obstante, otras limitaciones serían las anotaciones subjetivas y el llamado "estado de necesidad terapéutico". Considera que en este último límite se deberá dejar constancia en la historia clínica.

Respecto a las anotaciones subjetivas, coincide con la ACPD en distinguir entre "apreciación subjetiva" y "anotación subjetiva" (apreciaciones o intuiciones que tienen relación con la enfermedad). Se ha planteado quién quita las anotaciones subjetivas, si el departamento de gestión de la historia clínica o el médico: las Agencias consideran que si el departamento advierte una "anotación subjetiva" lo deberá comunicar al médico, y en todo caso, éste deberá comunicar porqué no se debe entregar la misma, ya que el derecho de reserva a no comunicarlas no es un derecho absoluto.

El público planteó las siguientes preguntas:

- Que los pacientes quieren conocer los profesionales que han accedido la historia clínica. La ACPD y APDCM consideran que el derecho de acceso no fundamenta conocer esa información, salvo que el propio Hospital quiera facilitarlo.
  La AVPD, inicialmente, en algún informe sí reconoció ese acceso, pero que actualmente ya no y lo reduce a conocer el número de personas, sin nombre y apellidos, que han accedido al historial médico.
- Acceso a los antecedentes familiares, ya que en algunos casos se da información especialmente sensible (por ejemplo, esquizofrenia del padre).

La APDCM respondió que tal y como ha planteado anteriormente debe haber un balance entre el interés del menor y el derecho del padre/madre.

CUARTA SESIÓN: Mejores prácticas para la mejora de la seguridad Iniciativa y proyectos



Realizó la introducción **Santiago Abascal Conde,** director de la APDCM.

Su intervención para introducir esta cuarta sesión giró en torno a las medidas de seguridad, que en el caso de los datos de salud, son de nivel alto, así como que todos aquellos que intervienen en el proceso evolutivo del paciente deben cumplir el deber de secreto, evitándose también el acceso masivo a la historia clínica.

En este sentido, manifestó que aun cuando la complejidad de la implantación de las medidas



de seguridad supone un importante esfuerzo para las organizaciones sanitarias, debe contemplarse, no como una carga, sino como una garantía de nuestros derechos constitucionales e incluso como una oportunidad de mejora en la prestación de los servicios asistenciales.
Además, la relación médico-paciente se basa en una doble confianza: en la competencia técnica y científica del profesional sanitario que nos atiende y, por otro lado, en que todo aquello que le confiamos en un acto médico, así como el resultado de las pruebas, las evaluaciones médicas, los diagnósticos, los tratamientos, la medicación o las recomendaciones que se nos hacen, quedan en la estricta confidencialidad de esta relación, relación que, aunque en nuestros modernos sistemas sanitarios no se reduce a un solo profesional, sino que se amplía y comparte entre todos aquellos que se ocupan de nuestra salud, sí ha de quedar confinada a aquellos que acceden y utilizan nuestros datos para prestarnos los servicios sanitarios que necesitamos.
Pues bien, en el momento actual, cuando cada vez son más los tratamientos de datos que se realizan de forma automatizada, y cuando se dispone de herramientas que permiten los accesos y tratamientos masivos de datos desde cualquier lugar y en cualquier momento, la preservación de ese bien indispensable de la confianza se produce exclusivamente desde dos premisas indispensables: el deber de secreto y la adopción de las necesarias medidas de seguridad.

Actuó de moderador **Ángel Igualada Menor,** subdirector de Registro de Ficheros y Sistema de las APDCM.

Introdujo la sesión presentando a los ponentes y haciendo mención de que todos ellos se encargan de la seguridad en sus respectivas organizaciones.

Pregunta 1. ¿Cómo se ha planteado la protección de datos y la seguridad de la información?

Manual Gimbert del Río (MGR), responsable de Seguridad de la Información del Hospital Reina Sofía, dijo que en su hospital los profesionales no solo están preocupados por la confidencialidad sino también por la integridad, de manera que se ha pasado de "hablar" de protección de datos a "hablar" de seguridad de la información. Pone como ejemplo de integridad, el cambio erróneo, sin intencionalidad, de una etiqueta sobre una prueba médica de un paciente. En este sentido, existen una serie de recomendaciones de la Organización Mundial de la Salud al respecto.
Asimismo, destacó que en su hospital el Responsable de Seguridad de la Información participa en algunas comisiones, como la de historia clínica.

Juan Miguel Signes Andreu (JMSA), responsable de Seguridad de la Información. Consejería de Sanidad. Agencia Valenciana de Salud, manifestó que en su caso, se han planteado la existencia de un "gobierno de la seguridad" en el cual se implique a los mandos directivos. Dio como ejemplo la elaboración de una política de seguridad.
Asimismo, el Gobierno Valenciano va a aprobar una política de seguridad aplicable a toda la Adminis-

tración pública de esa Comunidad Autónoma. Posteriormente, se aprobará una orden en el ámbito de la Consejería de Salud determinando las responsabilidades de cada uno de los agentes intervinientes.

José Manuel Laperal (JML), responsable de seguridad e innovación. Dirección General de Sistemas de Información Sanitaria del SERMAS, consideró que hay que "crecer" cada vez más hacia al conocimiento y formación de los profesionales, ya que la prevención es fundamental. A su juicio, la formación es la mejor herramienta para prevenir incumplimientos y además, supone prestar una gestión sanitaria de mayor calidad.

Pregunta 2. ¿Hasta qué punto están implantadas las medidas de seguridad y que colaboración existe con los centros de salud?

MGR.- Han realizado una campaña de formación que se ha impartido a un gran número de profesionales. En ocasiones, elaborando planes específicos, como por ejemplo, para el personal de admisión o el dirigido a los que se dedican a la atención al ciudadano.
En Andalucía, la Unidad de Gestión Clínica debe pasar una auditoria cada dos años y su Departamento se encarga de realizarlo en su Hospital.
JMSA.- Tanto el Reglamento de la LOPD como el ENS exigen un nivel de la seguridad muy "maduro". En otras palabras, un alto cumplimiento en materia de seguridad. En este sentido, existen controles de seguridad que se aplican en toda la organización –por ejemplo, la declaración de ficheros- que en la Comunidad Valenciana lleva a cabo la Consejería de Sanidad.
En cuanto al grado de colaboración de los centros está por debajo de lo que a él le gustaría, ya que algunos de ellos consideran que tienen un "estatus" de independencia.
JML.- la información, como puede ser el número de registros de accesos, debe estar en conocimiento no sólo de la Consejería de Sanidad sino también de los centros hospitalarios y de salud.
Respecto al riesgo, hay que trasladarlo también al centro de salud porque es donde están los profesionales, de manera que hay que hablar no sólo de la LODP sino de seguridad de la información.

Pregunta 3. ¿Cómo entendéis el concepto de fichero en el ámbito público y, sobre ese fichero, cómo se realiza el documento de seguridad y las auditorías?

MGR.- Considera que hay que simplificar: pone como ejemplo la existencia de un solo fichero de historia clínica. Ello no es impedimento para que se controle el acceso a la misma mediante el registro de accesos.
En cuanto a los documentos de seguridad, los aspectos formales del mismo son sencillos. Lo complicado es actualizarlo, difundirlo e implicar a los profesionales.
Respecto a las auditorías, han realizado bastantes desde el 2008.
JMSA.- A finales del año pasado re-organizaron la declaración de ficheros ante la AEPD. Asimismo, han "interpretado" la definición de fichero, dotándole de un grado de abstracción superior a la existencia de una aplicación informática. De esta forma, crearon 11 ficheros que ellos mismos llaman "jurídicos" a los cuales están vinculados los llamados ficheros "físicos" (las aplicaciones informáticas).
En cuanto a las auditorías las realizan sobre seguridad de la información, que son más amplias que las previstas a nivel LOPD.
JML.- En el año pasado suprimieron más de 1.000 ficheros en el ámbito sanitario, ya que tenían más de 4.000. Además, realizaron casi 1.000 auditorías. De esta forma, están realizando un proceso de racionalización, incluyendo la implantación de herramientas en los centros para que sea más sencillo.
Pregunta 4.- ¿Qué necesitan para cumplir con todas las obligaciones?
MGR.- Las herramientas son sencillas: planes de formación adaptados a cada sector. También "alineación" entre la seguridad de la información y la del paciente.
JMSA.- Han creado un sistema informático llamado "Línea básica de seguridad", que establece los controles de seguridad para cada tipo de tratamiento.
Asimismo, le gustaría que hubiese un cambio cultural en los profesionales que trabajan en los centros, de manera que pensasen que trabajan en una gran organización superando los llamados "reinos de taifas". De esta forma, el potencial sería mayor.
JML.- Hay que lograr una mayor presencia de los profesionales de la seguridad en el ámbito asistencial, como formar parte de la Comisión de Historias Clínicas. También debe haber una mayor implicación de los directivos en la seguridad.

Pregunta el público:
- ¿Realmente para cumplir la protección de datos en los centros hospitalarios falta personal?
- ¿Debe existir un régimen disciplinario específico ante el no cumplimiento de las medidas de seguridad?

MGR.- Que es necesario un responsable de seguridad que implique al resto de la organización para que la seguridad se cumpla.

JMSA.- El incumplimiento de la seguridad muestra que no existe un grado de madurez adecuado al respecto.

JML.- Considera que para cumplir la seguridad debe implicarse a la dirección.

QUINTA SESIÓN: Protección de datos y gestión de biobancos



La introduccióncorrió a cargo de **Iñaki Vicuña de Nicolás**. Director AVPD.
En el discurso de apertura de la última sesión hizo referencia al marco legal existente en esta materia, la Ley de Investigación Biomédica, que deja claro el "campo de juego" y, además, se centra en el elemento fundamental que son las personas.
Asimismo, citó que el objetivo de esta sesión es conocer en la práctica como funciona un biobanco.

Moderador.- **Pedro Alberto González**. Responsable del Registro de Ficheros y Nuevas Tecnologías. AVPD.

Pregunta 1. ¿Qué es un biobanco?

Roberto Bilbao Urquiola (RBU), coordinador General del Biobanco Vasco para la Investigación, habló sobre el biobanco, que garantiza la trazabilidad de una muestra biológica y el anonimato de la persona de la que se obtiene. Dicho anonimato se garantiza con un código de identificación.
Los usuarios de esos biobancos son todos aquellos que quieran realizar investigación.



Iñaki Vicuña de Nicolás

Asimismo, se nutren de la información de los pacientes: por ejemplo, una persona con un tumor, antes de ser operada se le pedirá el consentimiento informado para la investigación biomédica y, así, una parte de la muestra obtenida –la necesaria para la investigación- pasa al biobanco.
Cuando el investigador pide las muestras, previamente debe presentar un proyecto de investigación autorizado por el Comité de Bioética.

Manuel M. Morente (MMM), coordinador de la Red Nacional de Bancos de Tumores del Centro Nacional de Investigaciones Oncológicas, sin entrar en la definición, aludió a la existencia de una Red de Biobancos, ya que no hay país en el mundo ni hospital que sea capaz de dar respuesta a los retos existentes, de ahí que haya que asociarse.
También comenta que una Red de Biobancos no es propietaria de nada, y que se respeta toda la normativa, y que España tiene la red más competitiva, pero que habría que dar un valor añadido. Además, la red funciona como "una ventanilla única" para los investigadores.

Antonio Casado da Rocha (ACR), vicedecano de Investigación, Movilidad y Proyección Social de la Facultad de Filosofía, dijo que, en su opinión, la sociedad necesita investigar, sobretodo en época de crisis. Para ello es necesaria la colaboración de la ciudadanía para que facilite sus muestras biológicas.

Pregunta 2. ¿Y las personas? ¿Cómo están en relación a los biobancos?

ACR.- Citó dos casos famosos: a mediados de los años 90 un científico consiguió tener toda la información genética de los islandeses (hubo colaboración del gobierno de esa país con el investigador), lo cual supuso una gran polémica de manera que Islandia tuvo que aprobar una ley para regular los biobancos; y otro de una tribu india –los havasupai- a los que una Universidad tuvo que indemnizarlos por utilizar su información biomédica para una finalidad diferente de aquella para la que había sido recogida –en concreto, para determinar su ascendencia antropológica- y cuyos resultados chocaban frontalmente con su cosmología.
También resaltó la importancia de los biobancos ya que incluso la opinión de los ciudadanos sobre los mismos ha sido incluido en el Eurobarómetro. En dicha encuesta se muestra que la sociedad más favorable a colaborar dando muestras son los islandeses lo que demuestra que el debate y conocimiento público mejora la actitud de colaboración de los ciudadanos.
MMM.- Consideró que, en todo caso, los derechos del individuo están por encima de la colectividad y que deben ser respetados en todo momento. Sobre la cuestión de protección de datos opina que están discriminados en relación con otros sectores.
RBU.- Introdujo el tema del consentimiento informado precisando que no tiene nada que ver con el consentimiento informado existente en el ámbito sanitario. También cree que hay que sensibilizar a la sociedad sobre los biobancos, que su fin es servir a la sociedad a través de la investigación. Otro punto importante es lo referente al consentimiento informado, ya que hay que trabajar sobre la elaboración de documentos adecuados para que la información al particular sea perfectamente comprensible.
Se pregunta por los asistentes si existe una confianza en que los investigadores utilizarán la información adecuadamente.
RBU.- Cuando la muestra llega al biobanco ya llega anonimizada -que no disciada-, luego la vuelven a codificar para su envío al investigador. Obviamente éste tiene que usarlo para el fin solicitado, que no es otro que la investigación que viene abalada por el Comité Ético. Además, debe justificar el número de muestras que necesita.



E. Aced, L. Saez y P. A. González



Aspecto general de los asistentes



CLAUSURA

En el acto de clausura del Foro, **Emilio Aced Félez**, Coordinador del mismo, realizó un breve resumen de los temas y conclusiones más relevantes que se habían producido a lo largo de sus dos días de duración.

A continuación, **Luciano Sáez Ayerra,** Presidente de la SEIS, mostró su agradecimiento a las autoridades de protección de datos por su compromiso con el Foro y por resaltar su utilidad e importancia y al Gobierno de Navarra y SODENA por su colaboración y financiación que permiten la viabilidad del mismo.

Finalmente, **Carlos Fernández Valdivielso**, Director-Gerente de SODENA, resaltó la importancia del Foro de Protección de Datos para Navarra y, tras apostar por la continuidad de la iniciativa, declaró clausurado el mismo.



Solicitud de Ingreso en la Sociedad

Datos Personales

Apellidos

Nombre | Fecha de nacimiento | D.N.I./ Pasaporte | Sexo

Domicilio | Localidad

C. Postal | Provincia | Prefijo | Teléfono | Fax

Correo eléctronico | Página Web

Titulaciones

Titulación | Otra

Datos Profesionales

Nombre de la Empresa o Institución

Departamento / Sección | Cargo desempeñado en la actualidad

Domicilio | Localidad

C. Postal | Provincia | Prefijo | Teléfono | Fax

Correo eléctronico | Página Web

Datos de Domiciliación Bancaria de Pagos

Banca o Caja de Ahorros | Dirección de la Sucursal

Localidad de la Sucursal | C. Postal | Provincia

Entidad | Oficina | D.C. | Número de cuenta | Titular de la Cuenta

Les ruego que con cargo a mi cuenta (arriba indicada con 20 dígitos) atiendan hasta nuevo aviso las órdenes de pago (75 euros/año el primer año y 45 euros/año los sucesivos) que presente la SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD a nombre de

_____

____ / ____ / ____

Firma del Titular

NOTA: A devolver cumplimentado y firmado a:

CEFIC. Secretaría Técnica
C/ Enrique Larreta, 5 • Bajo Izda
28036 Madrid
Tlfno: 91 - 388 94 78 • Fax: 91 - 388 94 79
e-mail: inscripciones@cefic.es

De acuerdo con la Ley Orgánica 15/99, de 13 de diciembre sus datos de carácter personal están integrados en un fichero para su tratamiento automático según los principios establecidos de confidencialidad, integridad y disponibilidad de datos. Solicitamos su autorización para que tales datos sean utlizados por nosotros para su inscripción.

Fecha: Firma:



La Llave para Traspasar las Barreras de la HCE

InterSystems HealthShare™ es una plataforma estratégica de informática sanitária que conecta aplicaciones, desbloquea todos los datos, crea una vista Web de cada paciente, permite un desarrollo rápido de nuevas funcionalidades y ofrece información detallada basada en "active analytics" en tiempo real ya sea a nível hospitalario, regional o nacional.

InterSystems

InterSystems.es/Key2

© 2012 InterSystems Corporation. Todos los derechos reservados.
InterSystems HealthShare es una marca registrada de InterSystems Corporation.



El gurú de su empresa puede ser usted.

Planificar, anticiparse, innovar... A veces contar con un referente a la hora de tomar cualquier decisión puede ser tan importante como la capacidad de liderazgo. Pulso, disponible en versión para tablet multidispositivo, es una publicación creada para convertirse en guía de referencia en tecnologías de la información y las comunicaciones. Descárguese la aplicación y cuente con nosotros para ser su nueva fuente de inspiración.

Pulso. La revista de tendencias TIC para liderar.
App disponible para todos los sistemas operativos.

www.grandesclientes.telefonica.es
www.aunclicdelastic.com

Telefónica

pulso
TENDENCIAS TIC PARA LIDERAR