Plan de inspección sectorial de oficio Hospitales Públicos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Plan de inspección sectorial de oficio Hospitales Públicos

Índice

1. INTRODUCCIÓN

Uno de los nueve artículos del juramento hipocrático señala *"Lo que acaso en el ejercicio de la profesión, y aún fuera de ésta, viere u oyera acerca de la vida de las personas, y que no deba alguna vez ser revelado, callaré, considerándolo secreto."*

Este canon pone de manifiesto la importancia del escrupuloso respeto a la intimidad por parte de la profesión médica, resaltando la importancia de que las instituciones sanitarias garanticen la confidencialidad de la información relacionada con los servicios que prestan, así como, en un sentido más amplio, la protección de los datos personales de los pacientes.

Debe tenerse en cuenta que los datos de salud se encuentran incluidos en el Reglamento General de Protección de Datos (RGPD), que será aplicable el 25 de mayo de 2018, entre los denominados como categorías especiales de datos, cuyo tratamiento se caracteriza por exigir garantías reforzadas.

Por otro lado, los tratamientos de datos de salud se enfrentan hoy a una revolución digital en la que la cantidad de datos que se acumulan sobre las personas crece enormemente y con una conectividad sin precedentes. Todo ello plantea nuevos retos para la protección de datos de carácter personal, más aún cuando el acceso a la Historia Clínica y su compartición entre diferentes instituciones sanitarias se considera imprescindible para prestar una mejor asistencia médica.

El análisis de la adecuación a la legislación vigente de estos tratamientos a gran escala de datos sensibles ha llevado a que, dentro del Plan estratégico 2015-2019 de la Agencia Española de Protección de Datos, en el Eje estratégico 1 denominado "Prevención para una protección más eficaz", se contemple un programa dedicado a la Sanidad, donde se engloba el presente Plan Sectorial de Oficio, que se centra en los procedimientos técnicos y políticas de actuación de los hospitales públicos, valora su nivel de adecuación a las previsiones de la normativa de protección de datos y emite recomendaciones con el objetivo final de elevar el nivel de cumplimiento del sector en esta materia, así como generar confianza en las actuaciones de las instituciones sanitarias tanto en el ámbito asistencial como en el de la investigación.

2. LEGISLACIÓN APLICABLE

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (**LOPD**).
- 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 (**RDLOPD**).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos (**RGPD**), aplicable a partir de mayo de 2018.
- 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 (**LAP**).
- Ley 14/1986, de 25 de abril, General de Sanidad.
- Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud
- Ley 33/2011, de 4 de octubre, General de Salud Pública.
- RD 1090/2015, de 4 de diciembre, por el que se regulan los Ensayos Clínicos con Medicamentos, los Comités de Ética de la Investigación con medicamentos (CEIm) y el Registro Español de Estudios Clínicos (**RD-ECM**).
- REGLAMENTO (UE) 536/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre los Ensayos Clínicos de Medicamentos de uso humano (**RUE-ECM**).
- Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.

También hay que tener en cuenta las recomendaciones recogidas en el Código de Conducta denominado Código Tipo de Farmaindustria, de la Asociación Nacional Empresarial de la Industria Farmacéutica establecida en España.

3. ACTUACIONES REALIZADAS

En el año 1995, la Agencia Española de Protección de Datos diseño un Plan Sectorial de Oficio con el objeto de analizar el nivel de adecuación a la normativa de protección de datos en el sector de la asistencia hospitalaria pública.

A partir del Catálogo Nacional de Hospitales, publicado por el entonces Ministerio de Sanidad y Consumo, se realizó un estudio previo de hospitales públicos atendiendo al número de camas, la finalidad asistencial (General, Quirúrgico, Maternal, Infantil, Materno-Infantil, Psiquiátrico, Enfermedades del Tórax, Oncológico, Traumatología y/o rehabilitación, Geriatría y larga estancia y Otras) y a su dependencia funcional, realizándose la selección de hospitales a visitar atendiendo a varios criterios: dependencia funcional (Sistema Nacional de Salud, Defensa, Justicia), número de camas y ubicación geográfica. Dentro de estos criterios la muestra de hospitales a inspeccionar se escogió de forma aleatoria.

Realizadas las inspecciones correspondientes, las actuaciones finalizaron el año 1996 con la elaboración de un informe de conclusiones que ponía de manifiesto las deficiencias detectadas, que de forma resumida fueron:

- No se informaba a los afectados de los puntos indicados en el artículo 5 de la Ley de Protección de Datos.
- No existían procedimientos para ofrecer información a los afectados ante el ejercicio de su derecho de acceso.
- No existía el necesario conocimiento e implicación por parte de los órganos directivos de los centros, en lo que a protección de datos se refiere, así como tampoco una mentalización adecuada respecto de los problemas de seguridad.
- No existían definiciones de nivel de confidencialidad de los datos que se utilizan desde los distintos puntos de tratamiento de los centros.
- No estaban definidos ni documentados los procedimientos en materia de cesión de datos médicos ni los requisitos legales necesarios para su cesión a otros centros.
- No existían procedimientos sobre los tipos de datos que pueden transferirse internacionalmente así como los posibles destinatarios.
- No existía control de salida de datos de los centros.
- No existía un Plan de Seguridad ni conciencia respecto de los riesgos asociados a una seguridad deficiente.

Posteriormente, en el año 2010, esta Agencia realizó un seguimiento mediante un cuestionario remitido a todos los hospitales del Catálogo Nacional para analizar el cumplimiento de la normativa de protección de datos, incluida la implementación de las medidas de seguridad sobre los datos personales tratados, obteniéndose un informe de situación que reportaba las principales carencias en:

- las cláusulas informativas de los formularios de recogida de datos,
- los carteles informativos sobre protección datos,
- la disponibilidad de procedimientos para atender el ejercicio de los derechos ARCO,
- las revisiones del documento de seguridad,
- el registro de los accesos a los datos,

- la seguridad en el almacenamiento de las historias clínicas en papel para evitar accesos no autorizados, así como la adopción de medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte,
- en general, en la implantación de medidas de seguridad y su auditoría periódica.

En general se detectó una evolución positiva en el sector con relación al cumplimiento de la normativa de protección de datos.

Según figura en el Catálogo Nacional de Hospitales 2016 del Ministerio de Sanidad, Servicios Sociales e Igualdad, España tiene 791 hospitales, de los cuales 357 son públicos y 434 son de propiedad privada, para cubrir las necesidades sanitarias de aproximadamente los 47 millones de habitantes que viven en el territorio nacional.

Dentro de las formas de gestión pública en sanidad se encuentran dos modelos, el primero de ellos es la gestión directa o prestación del servicio público directamente por medio de la Administración, aunque sea con una persona jurídica interpuesta, y la gestión indirecta, en la que la prestación del servicio público es realizada por el sector privado, manteniendo la Administración Pública la provisión del servicio público mediante alguno de los tipos de contratación externa establecidos en el Texto Refundido de la Ley de Contratos de las Administraciones Públicas (TRLCAP), Ley 53/1999 o en la misma LGS de 1986.

HOSPITALES POR COMUNIDAD AUTÓNOMA Y DEPENDENCIA PATRIMONIAL

Comunidad Autónoma	Seguridad Social	Administración Central	Ministerio de Defensa	Comunidad Autónoma	Diputación o Cabildo	Municipio	Entidades Públicas	MATEP	Privado Benéfico (Cruz Roja)	Privado Benéfico (Iglesia)	Otro Privado Benéfico	Privado no Benéfico	TOTAL
ANDALUCÍA	2	1	0	43	0	0	0	1	2	7	0	52	108
ARAGÓN	7	0	1	11	0	0	1	1	0	2	0	6	29
PPDO. DE ASTURIAS	6	0	0	2	0	0	1	0	1	1	3	6	20
ILLES BALEARS	4	0	0	4	3	0	0	1	1	1	0	10	24
CANARIAS	2	0	0	7	5	1	0	0	0	1	1	21	38
CANTABRIA	3	0	0	0	0	0	0	1	0	2	0	1	7
CASTILLA Y LEÓN	4	0	0	1	1	1	8	0	1	7	4	9	36
CASTILLA-LA MANCHA	11	0	0	7	1	0	0	1	0	0	0	8	28
CATALUÑA	9	0	0	27	1	11	19	5	3	17	42	80	214
COMUNIDAD VALENCIANA	17	1	1	14	3	0	0	2	0	1	2	20	61
EXTREMADURA	3	0	0	3	0	1	4	0	0	1	0	7	19
GALICIA	4	0	0	3	0	0	7	1	0	0	2	21	38
MADRID	12	0	2	20	0	0	0	2	1	11	2	31	81
REGIÓN DE MURCIA	6	0	0	4	0	1	0	1	0	0	2	13	27
C. FORAL DE NAVARRA	0	0	0	4	0	0	0	0	0	3	2	2	11
PAÍS VASCO	3	0	0	14	0	0	0	2	1	4	2	15	41
LA RIOJA	1	0	0	4	0	0	0	0	0	0	0	2	7
CEUTA	1	0	0	0	0	0	0	0	0	0	0	0	1
MELILLA	1	0	0	0	0	0	0	0	0	0	0	0	1
TOTAL NACIONAL	96	2	4	168	14	15	40	18	10	58	62	304	791

Los Complejos Hospitalarios se contabilizan como un solo hospital

Durante el año 2016, esta Agencia ha realizado nuevas actuaciones de inspección dirigidas a los centros hospitalarios de titularidad pública −teniendo en cuenta los gestionados tanto de forma directa como indirecta−, centrándose en la auditoría de los aspectos con más carencias detectadas en las actuaciones anteriores, en concreto, en

las medidas de seguridad implementadas, con visitas presenciales a los hospitales que fueron inicialmente auditados y hospitales de nueva creación.

Así, se han auditado hospitales públicos de gestión directa e indirecta entre los que se encuentran:

- Hospitales que, partiendo de una situación de Historia Clínica en papel, la han automatizado a formato electrónico.
- Hospitales que conservan todavía la Historia Clínica de sus pacientes en papel y que están inmersos en distinta medida en procesos de automatización de la documentación médica.
- Hospitales de nueva creación, con Historia Clínica Electrónica desde su nacimiento.

Con respecto a los servicios hospitalarios inspeccionados, la selección se ha realizado atendiendo a los tratamientos de datos personales que realizan, con especial atención a los relativos a datos especialmente protegidos. Entre los servicios auditados se encuentran: Admisión, Urgencias, Consultas Externas, Anatomía Patológica, Unidad de Cuidados Intensivos, Laboratorio de Análisis Clínicos, Farmacia Hospitalaria, Departamento de Informática, Atención al Paciente, Servicios Sociales y Biobanco.

Por otro lado, en los hospitales se realizan tratamientos de datos personales con dos finalidades diferentes:

- asistencial, encaminada a prestar asistencia sanitaria a los pacientes que acuden al centro, y
- de investigación médica, cuyo objetivo es generar nuevos conocimientos que ayuden al diagnóstico, tratamiento y prevención de las enfermedades.

Por ello, en varios de los hospitales auditados se han realizado también comprobaciones in situ sobre los procedimientos de investigación médica y los tratamientos de datos personales que se efectúan en este ámbito.

A continuación se describen los modelos de gestión de datos, las conclusiones y recomendaciones de forma separada para el ámbito asistencial y para el de investigación médica.

4. DESCRIPCIÓN DEL MODELO DE GESTIÓN DE DATOS EN EL ÁMBITO ASISTENCIAL

4.1. HISTORIA CLÍNICA

El art. 3 de la LAP define la Historia Clínica (HC) de un paciente como el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

Su finalidad es garantizar una adecuada asistencia médica al paciente y debe llevarse con criterios de unidad e integración al menos en cada institución asistencial. Incluye un conjunto de documentos organizados de forma secuencial relativos a los procesos asistenciales de cada paciente, incluyendo datos sobre su situación y evolución clínica que hacen referencia a sus episodios de salud y enfermedad, y a la actividad sanitaria que se genera con motivo de estos episodios, con identificación de los médicos y demás profesionales que han intervenido en ellos.

La historia clínica electrónica (HCE) supone utilizar las Tecnologías de la Información y las Comunicaciones (TIC) en la actividad sanitaria, almacenando la información generada de forma digital, lo que facilita su integración en un Sistema de Información Clínica, normalmente denominado HIS por sus siglas en inglés (*Healthcare Information Systems*).

Se puede considerar a la HCE como la versión digital de la HC, como un registro unificado y personal, de contenido multimedia, archivado en soporte electrónico.

En general, los datos médicos incluidos en las HC tienen su origen en los informes de las asistencias que realizan los profesionales sanitarios al atender al paciente, así como los resultados e informes derivados de las diferentes pruebas a las que ha sido sometido.

Aunque en términos generales las Administraciones Sanitarias públicas han asumido una apuesta firme por la HCE que debe valorarse positivamente, en la actualidad coexisten en España hospitales con diferentes grados de automatización de la HC, existiendo centros que utilizan HC en formato papel, o en papel y con ciertos informes automatizados, hasta centros relativamente recientes que han tenido desde su nacimiento toda la HCE, si bien siempre, al menos en el momento actual, conservan en papel determinados documentos como pueden ser los consentimientos informados para las intervenciones quirúrgicas, para los procedimientos diagnósticos y terapéuticos invasores u otros procedimientos que así lo exijan.

Hay que indicar que, además de los sistemas de HC de los hospitales, existen Sistemas de HCE en los Servicios de Atención Primaria de las Comunidades Autónomas, que no son objeto de este estudio. Tanto los Sistemas de HCE de los hospitales como los de Atención Primaria no están a priori concebidos para ofrecer información cuando el paciente debe ser atendido fuera del ámbito geográfico donde su información se ha generado, si bien dentro de cada Comunidad Autónoma suele existir cierta compartición de información, según el grado de integración de los

diferentes Sistemas de HCE de los distintos Hospitales y Atención Primaria de la Comunidad Autónoma.

Existe también un proyecto de HCE del Sistema Nacional de Salud (HCDSNS – Historia Clínica Digital del Sistema Nacional de Salud), liderado por el Ministerio de Sanidad, Servicios Sociales e Igualdad, en colaboración con Red.es, las 17 Comunidades Autónomas y el Instituto Nacional de Gestión Sanitaria, cuyo objetivo es garantizar el acceso a la documentación clínica más relevante (HC resumida) para la atención sanitaria de los ciudadanos en sus desplazamientos por el territorio nacional. Se define el concepto de HC resumida como el conjunto mínimo de datos personales de salud que sean de interés para los profesionales sanitarios y cuya ignorancia podría suponer un riesgo para la salud del ciudadano asistido.

La HCDSNS no se compone de los documentos habituales de la práctica clínica, tales como informes, sino de datos estructurados facilitados por los Servicios de Salud de las Comunidades Autónomas como un Conjunto Mínimo de Datos (CMD), que incluye, entre otros, los siguientes: alergias, vacunaciones, problemas resueltos, cerrados o inactivos, problemas y episodios activos, y tratamientos.

El conjunto mínimo de datos se encuentra recogido en el Real Decreto de Conjunto Mínimo de Informes y Documentación Médica (RDCMDIC). El RDCMDIC es el que establece el conjunto de datos e información médica que se debe compartir.

Se puede acceder a la HC resumida a través de la HCDSNS en modo consulta. En abril de 2017 la cobertura de población que alcanza este sistema asciende al 78,32% de los ciudadanos con Tarjeta Sanitaria.

Por último, existe un proyecto europeo denominado epSOS, cofinanciado por la Comisión Europea, cuyo objetivo es el intercambio transfronterizo de datos de salud para mejorar la atención sanitaria de los ciudadanos cuando están fuera de su país. En un futuro, permitirá a los profesionales de la salud de cualquier país participante en epSOS acceder a los datos de HCE de los pacientes.

Por tanto, la evolución de la HC en el Sistema de Salud ha pasado por distintas fases, desde un primer conjunto de documentos en papel, con las dificultades de acceso y almacenamiento que conlleva, a una automatización parcial en la que conviven determinados archivos de documentos en papel con documentación médica automatizada, con el objetivo de llegar a una HC totalmente automatizada, de mayor disponibilidad, y que conlleva la mejora de los procesos de gestión clínica y de la atención a los pacientes. Finalmente, los nuevos proyectos HCDSNS y epSOS están encaminados a facilitar el acceso a datos médicos que residen en sistemas diferentes en distintas Comunidades Autónomas y Estados miembros de la Unión Europea.

4.2. SISTEMAS DE INFORMACIÓN HOSPITALARIOS

Los sistemas HIS nacieron con el objetivo de almacenar únicamente los datos administrativos de las instituciones hospitalarias relacionados con la gestión de los pacientes como usuarios del hospital, y han ido evolucionando hasta integrar los datos administrativos con los datos clínicos, es decir, aquellos que hacen referencia al estado de salud o de enfermedad de los pacientes, y que se recogen en su HCE.

Los Centros Hospitalarios Públicos son instituciones grandes con una gran cantidad de empleados y múltiples departamentos. Los Hospitales denominados terciarios integran:

- un nivel primario donde se atienden las consultas ambulatorias habituales de baja complejidad,
- un nivel secundario con las especialidades y recursos diagnósticos habituales (imágenes médicas y radiodiagnóstico, anatomía patológica, laboratorio de análisis clínicos, farmacia, urgencias, etc.)
- y un nivel terciario, con especialidades más complejas y de referencia tanto para la Comunidad Autónoma como para el ámbito estatal.

Los grandes Hospitales Públicos suelen ser multicentro, constando el complejo hospitalario (campus) de varios edificios. Además suelen contar con Centros de Especialidades descentralizados. Todos estos edificios e instalaciones comparten la misma red informática y el mismo Sistema de Información.

Suelen constar además de una zona no asistencial como Hospital Universitario, donde se imparten Grados Universitarios y de Formación Profesional.

En la actualidad, todos los hospitales disponen de un complejo Sistema de Información que se encuentra principalmente ubicado en su Centro de Proceso de Datos, dotado con una serie de servidores centrales en los cuales se encuentran instaladas la mayoría de aplicaciones con datos personales utilizadas por el personal sanitario, incluido el HIS.

Según el grado de implementación de la Historia Clínica Electrónica (HCE) este sistema central es más o menos completo e integra en mayor o menor medida los elementos auxiliares del Hospital, siendo estos básicamente los comúnmente denominados LIS (Sistema de Información Laboratorio), RIS (Sistema de Información de Imágenes médicas) y PHIS (Sistema de Información de la Farmacia Hospitalaria).

El RIS está siempre asociado a un PACS (Sistema de archivo y comunicación de imágenes médicas). Mientras que el RIS constituye el Sistema de Información del servicio, incluyendo todo el flujo de trabajo desde la introducción de la orden hasta la distribución de los resultados, los PACS permiten el almacenamiento y distribución de las diversas imágenes médicas: radiografías convencionales (RX), ecografías, resonancias magnéticas (RM), Tomografía Axial Computerizada (TACS), etc. Emplean para ello formatos de imagen estándares del sector.

Adicionalmente, estos sistemas conviven con un importante número de aplicaciones departamentales específicas que permiten a los departamentos tratar los datos

obtenidos de los pacientes y elaborar informes de las actuaciones que practican, si bien la mayoría de los Centros tienen implementado un modelo centralizado en el que las aplicaciones se instalan y administran en los servidores ubicados en el centro de proceso de datos, y los usuarios acceden remotamente a las aplicaciones desde sus puestos de trabajo.

También, para evitar que los diferentes departamentos tengan en ordenadores personales determinados ficheros ofimáticos con datos relativos a la salud de sus pacientes, en los servidores centrales se suelen crean espacios de almacenamiento con esta finalidad.

Esta centralización de la información es la tendencia actual y tiene repercusiones positivas para la protección de datos, ya que en la situación anterior de descentralización, que aún persiste en algunos casos, el control de la implementación de las medidas de seguridad es mucho más complejo.

Las aplicaciones informáticas se pueden dividir en tres categorías según su origen:

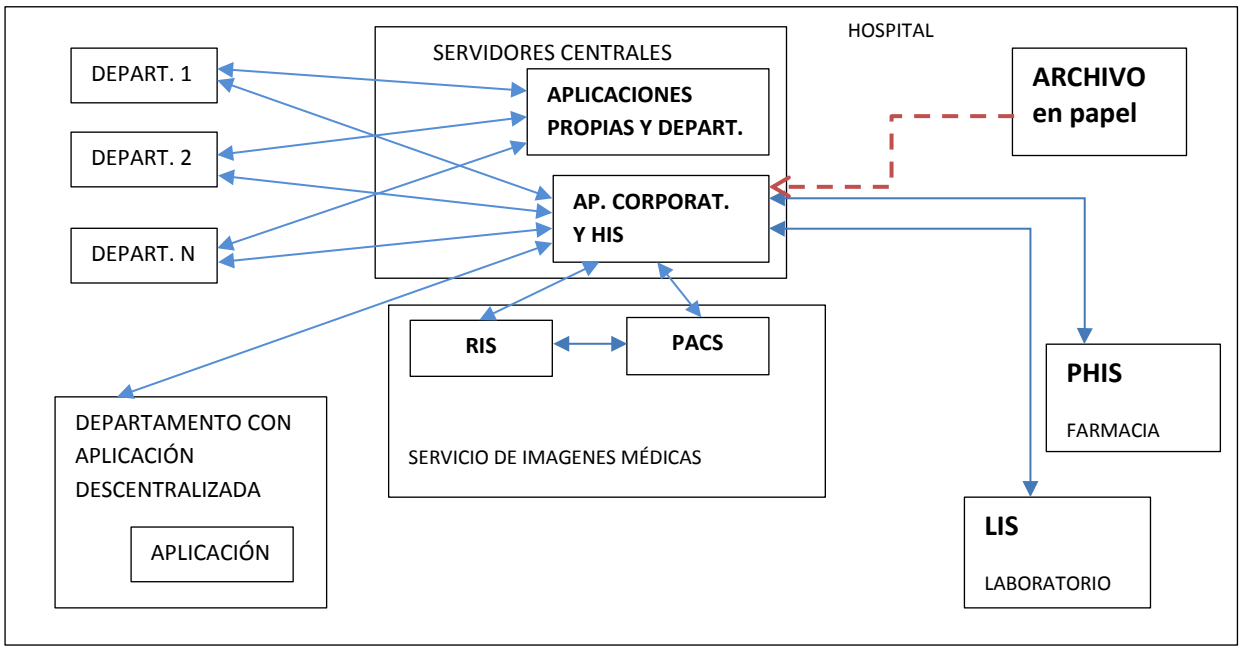
- Aplicaciones Corporativas, proporcionadas por la Consejería de Sanidad de la Comunidad Autónoma. Normalmente en este grupo se incluye el HIS para el tratamiento de los datos administrativos y, según su grado de implantación, de HCE.
- Aplicaciones Propias, desarrolladas a instancias del propio hospital, que son utilizadas por varios servicios.
- Aplicaciones Departamentales, desarrolladas por terceros, que utiliza un servicio para una gestión específica. Estas aplicaciones departamentales residen en los servidores centrales del centro de proceso de datos, pero ocasionalmente pueden encontrarse distribuidas en los distintos departamentos, aunque como se ha indicado la tendencia observada es la centralización, detectándose un esfuerzo muy importante en el sector para esta centralización y normalización de las aplicaciones.

En algunos casos, la administración de las aplicaciones departamentales, incluida la gestión de usuarios, se realiza por terceras entidades con las que se ha suscrito un contrato de prestación de servicios.

Los datos, informes y resultados de pruebas generados con las aplicaciones departamentales o auxiliares, incluidas las imágenes médicas, son normalmente accesibles desde el Sistema de Información que gestiona la HC general del hospital, comunicándose las aplicaciones departamentales con la aplicación de HCE mediante una mensajería estándar específica para el sector (HL7: conjunto de estándares para el intercambio de información clínica). Por medio de estos protocolos estándar se consigue que aplicaciones informáticas con tecnologías diferentes sean capaces de intercambiar información. Así, es posible almacenar información procedente de departamentos como Anatomía Patológica o Imágenes Médicas en la aplicación de la HCE y ponerla a disposición del personal médico autorizado.

Los datos pueden residir únicamente en una aplicación departamental, como normalmente es el caso de las imágenes médicas, o pueden almacenarse tanto en la aplicación departamental como en la general de HC del Hospital, generándose en este caso varias réplicas (normalmente parciales) de datos en distintas aplicaciones informáticas.

En el gráfico siguiente se puede observar la estructura básica típica de un Sistema de Información de un hospital.



Por otro lado, existen hospitales que todavía mantienen la HC en papel, si bien se espera que a medio plazo se proceda a la digitalización de todos ellos, dependiendo de los calendarios fijados por las diferentes Comunidades Autónomas. En los hospitales que mantienen la HC en papel, es habitual la existencia de una aplicación informática para la gestión de los datos básicos de los pacientes (HIS antiguo para el tratamiento de datos médico-administrativos únicamente, sin HCE) así como Sistemas de Información automatizados para los elementos auxiliares descritos (LIS, RIS y PHIS).

En los hospitales que mantienen la HC en papel, todos los documentos clínicos procedentes de los distintos departamentos se van incluyendo en las HC de los pacientes según se van generando.

Incluso en los hospitales que ya han implementado la HCE, suele pervivir un archivo en papel para el almacenamiento de documentación que todavía no ha sido escaneada o que por otras necesidades necesita ser conservada, como los consentimientos informados en papel ya comentados o documentos relacionados con nacimientos, incluidos los resultados de las pruebas biométricas, médicas o analíticas que resulten necesarias para determinar los vínculos de filiación con la madre.

También existen visores, que son aplicaciones informáticas que permiten la consulta de múltiple información de un paciente extraída de las diversas aplicaciones departamentales del hospital (e incluso de varios hospitales y Centros de Atención Primaria a nivel de Comunidad Autónoma), si bien estos visores, como su nombre indica, no permiten la modificación de los datos, únicamente su visualización.

Los complejos hospitalarios están interconectados con Centros de Atención Primaria y Centros de Especialidades. En estos centros no suele haber instaladas aplicaciones ni servidores departamentales, accediendo en su caso *online* a los sistemas centrales del

hospital y a aplicaciones específicas de Atención Primaria de la Consejería de Sanidad de la correspondiente Comunidad Autónoma. Para la interconexión de estos centros se utilizan redes privadas virtuales que proporcionan un medio de cifrado de la información y evitan que los datos de salud circulen por redes públicas de datos.

A determinados cargos de responsabilidad y otros profesionales autorizados se les habilita acceso remoto a su puesto de trabajo para controlar determinados aspectos de forma continuada. Este acceso se realiza a través de túneles de cifrado que permiten trabajar con el mismo entorno que si estuvieran en el hospital, evitando que el usuario tenga que descargar o transferir información relativa a los pacientes a su ordenador privado.

4.3. TRATAMIENTOS DE DATOS

Los datos de los pacientes se tratan o recaban por primera vez cuando acuden al hospital o los centros asociados por una de las siguientes vías:

- **Derivado desde Atención Primaria**

  Los hospitales cuentan con centros de Atención Primaria adscritos encontrándose en ellos las consultas de los médicos de familia que, en su caso, solicitan la realización de determinadas prestaciones médicas que se realizan en el hospital: procedimientos diagnósticos y terapéuticos, así como consultas de especialistas.

  En esta atención especializada, el paciente debe acudir al hospital en la fecha y hora indicada en la cita que se le asigna, sin que como norma general se pida acreditar nuevamente su identidad. Cuando el paciente acude a la consulta de especialidad del Hospital, sus datos personales ya han sido tratados en el centro de Atención Primaria (previamente recabados y extraídos de las bases de datos de filiación de las Consejerías de Sanidad), no pudiendo un paciente acceder a las consultas de especialidad sin pasar previamente por Atención Primaria.

- **Admisión desde Urgencias**

  Cuando un paciente llega a urgencias en un hospital, con carácter general, se le solicita su tarjeta sanitaria en la ventanilla de admisión. En caso de no llevarla se le solicita un documento oficial de identidad (DNI, NIE, pasaporte, etc.)

  No obstante, existe la obligatoriedad de prestar atención sanitaria en situaciones de gravedad y urgencias, también a pacientes indocumentados, por lo que todas las personas son atendidas aunque no presenten ningún documento. También pueden ingresar personas desorientadas o inconscientes a las que se asigna una identidad provisional hasta que se puede acreditar su identidad. Esta identificación provisional consiste en un código único que se utiliza en la HC provisional que se abre mientras está en urgencias.

  Una vez identificado el paciente, si no tiene todavía Historia Clínica (HC en papel o HCE) en el Centro, con la documentación que aporta se consulta la base de datos de la Consejería correspondiente, que contiene datos de filiación

de los habitantes, para descargar los datos permanentes como apellidos, fecha de nacimiento, etc., abriéndose una HC nueva en la que se almacenarán sus datos de salud. Los datos que figuran en la base de datos poblacional y que pueden haber variado, tales como la dirección o el teléfono, se confirman directamente con el paciente.

En caso de no residir en la Comunidad en que se encuentra el hospital, se extraen los datos del documento de identidad y de la información facilitada por el paciente, aunque se consulta la base de datos del Sistema Nacional de Salud (SNS) por medio del CIP de la tarjeta sanitaria.

Las tarjetas sanitarias son emitidas por las Comunidades Autónomas que dotan a cada persona tenedora de tarjeta de un Código de Identificación Personal propio de cada ámbito territorial (CIPA, o CIP-Autonómico). Este código tiene como principal cometido asegurar la asociación biunívoca de la persona con su información administrativa y clínica dentro de cada Comunidad Autónoma. Cada Comunidad Autónoma dispone de una base de datos de tarjetas sanitarias que contiene los registros de los ciudadanos protegidos en su ámbito.

El SNS tiene a su vez una base de datos común de tarjetas sanitarias que recoge la información de las bases de datos autonómicas, asumiendo el Ministerio de Sanidad y Consumo la competencia de asignar un Código de Identificación Personal (CIP) único y vitalicio a través de esta base de datos común, y sus vínculos con cuantos otros CIPA pueda tener cada ciudadano en los distintos territorios del Estado.

Si el paciente es menor de edad o incapacitado, se recaban los datos de los padres o tutores y se incorporan en el sistema de información.

A raíz de las actuaciones de inspección realizadas sobre el sector se han detectado tratamientos y aspectos relacionados con la protección de los datos de los pacientes que pueden ser mejorados.

Los datos de salud de los pacientes se encuentran en las HC y en diversos ficheros departamentales en los que, por la especificidad de los tratamientos que se realizan (diagnóstico por imagen, analíticas de anatomía patológica, etc.) sólo son accesibles a nivel departamental, generándose informes y resúmenes que se incluyen posteriormente en la historia clínica.

Se ha encontrado que, dependiendo de los centros auditados, las HC están en diferentes estados de automatización. Sobre las que se encuentran en papel se controla exhaustivamente el acceso al dosier y su ubicación, pero conllevan inconvenientes de seguridad en su transporte y almacenamiento durante el préstamo, así como a la hora de evitar el acceso indebido a la información que contienen o asegurar su integridad. Por otro lado, las historias clínicas electrónicas permiten el acceso a todo el personal médico, en ocasiones sin suficiente restricción.

A la hora de redactar estas recomendaciones se han diferenciado las dos principales finalidades en los tratamientos de datos que se han identificado en los centros hospitalarios auditados: asistencial y de investigación médica.

Seguidamente se detallan las conclusiones para las finalidades asistenciales.

4.4. CONCLUSIONES Y RECOMENDACIONES PARA FINALIDADES ASISTENCIALES

4.4.1. CONCLUSIÓN art. 4.3. LOPD - Calidad de los datos

En la mayoría de los centros inspeccionados no se verifica la identidad del paciente requiriendo el Documento Oficial de Identidad junto con la tarjeta sanitaria. Esto da lugar a que se produzcan casos de suplantación de identidad que, si bien son muy escasos, pueden suponer un alto riesgo para la salud de los pacientes, ya que la información contenida en la HC a la que se accede con la tarjeta sanitaria presentada no corresponde a la patología del paciente. Estos casos de suplantación se detectan normalmente por ser incongruente la información que contiene la HC con la patología del paciente, por ejemplo: partos consecutivos, operaciones que no se han realizado, etc.

RECOMENDACIÓN

Se debe solicitar un documento oficial de identidad junto con la tarjeta sanitaria que permita identificar correctamente al paciente.

En caso de que el paciente no muestre ningún documento identificativo, siempre que se deba prestar la asistencia médica inicial o de urgencias de forma obligatoria, se aplicará un protocolo, que deberá establecerse previamente, encaminado a la acreditación posterior de la identidad del paciente que permita la correcta incorporación de los datos de la asistencia en la HC correspondiente.

4.4.2. CONCLUSIÓN art. 4.5. LOPD 8.6 RDLOPD - Cancelación y borrado de los datos. Art.17 LAP

Con carácter general, en los hospitales visitados no está previsto un mecanismo de borrado, cancelación o bloqueo de datos, almacenándose información desde el día en que se puso en producción, entendiendo que la HC no debe ser eliminada por motivos asistenciales. Tampoco se destruyen las HC en papel.

Por otro lado, se han encontrado tratamientos concretos, tales como las listas de espera quirúrgicas o las derivaciones entre hospitales, en las cuales se mantiene una base de datos con fines administrativos. Esta base de datos contiene toda la documentación relacionada, que puede incluir datos de salud, habiéndose detectado que no se ha ejecutado hasta la fecha ningún protocolo de eliminación de datos.

RECOMENDACIÓN

La documentación clínica debe ser conservada durante el tiempo necesario para prestar la debida asistencia al paciente y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial. En caso de que la Comunidad Autónoma haya aprobado legislación específica que contemple periodos mínimos de conservación más largos, deberán ser tenidos en cuenta.

La información utilizada para fines administrativos, tal como la utilizada para la gestión de las listas de espera o las derivaciones entre hospitales, tras ser incorporada a la HC y dejar de ser necesaria para la gestión administrativa, debe ser destruida.

Por otro lado, tal cual se especifica en la LAP, los datos de la HC relacionados con el nacimiento del paciente, incluidos los resultados de las pruebas biométricas, médicas o analíticas que en su caso resulten necesarias para determinar el vínculo de filiación con la madre, no se destruirán.

4.4.3. CONCLUSIÓN art. 5. LOPD - Información

Se ha comprobado que varios de los hospitales visitados no tienen carteles informativos en las áreas donde se recaban datos de los pacientes (por ejemplo, en Admisión o Urgencias), no informándose tampoco verbalmente o por escrito sobre los derechos de protección de datos de los pacientes y usuarios del centro.

Si bien algunos centros hospitalarios sí disponen de carteles informativos sobre los derechos de los pacientes a ser informados, estos no recogen todos los aspectos previstos en el artículo 5 de la LOPD, al estar más alineados con 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, o al tener referencias obsoletas, por ejemplo a la Agencia de Protección de Datos de la Comunidad de Madrid.

RECOMENDACIÓN

Aunque la legislación habilita el tratamiento de los datos para la prevención o el diagnóstico médico o prestación de una asistencia sanitaria por personal sanitario sujeto a secreto profesional sin necesidad de recabar el consentimiento, es necesario informar en la recogida de los datos de los aspectos recogidos en el art. 5 de la LOPD, y en concreto, de la forma de ejercitar los derechos ARCO.

Se considera conveniente elaborar y situar en lugar visible, al menos en las áreas de Admisión y Urgencias, carteles informativos sobre la identificación del responsable del fichero, el modo de ejercitar los derechos ARCO y de la dirección o departamento al que deben dirigirse para ello.

En los formularios que sean utilizados para la recogida de información de los pacientes y usuarios, así como en los consentimientos informados que deben firmar para la realización de determinadas intervenciones y pruebas diagnósticas, deberán incluirse cláusulas informativas y adaptadas a cada formulario, que incluyan la información prevista en el apartado 1 del artículo 5 de la LOPD.

El Reglamento General de Protección de Datos será aplicable a partir de mayo de 2018, pero es aconsejable que los hospitales vayan adaptando sus políticas informativas a lo dispuesto en el mismo, ya que incluye nuevas obligaciones en relación a la información a facilitar a los interesados. Se recomienda que la información exigida en el nuevo Reglamento que pueda ya anticiparse se incorpore a la que en la actualidad se proporciona, realizando una adaptación progresiva.

En este sentido, se podrían ir introduciendo en la información facilitada detalles como los siguientes:

- Los datos de contacto del Delegado de Protección de Datos cuando este sea designado.
- La base jurídica o legitimación para el tratamiento.
- El plazo o los criterios de conservación de la información.
- La existencia de decisiones automatizadas o elaboración de perfiles.
- La previsión de transferencias a terceros países.
- El derecho a presentar una reclamación ante la Autoridad de Control.

En este sentido, la Agencia Española de Protección de Datos ha elaborado una Guía para el cumplimiento del deber de informar según el nuevo Reglamento.

4.4.4. CONCLUSIONES art. 10 LOPD - Deber de secreto

A. CONCLUSIÓN

No todos los hospitales que gestionan la HC en papel han establecido en normas internas que se trata de documentación confidencial, especificando que todo el personal que tiene acceso a la HC, bien para su consulta a nivel asistencial (personal sanitario) o para su consulta para fines administrativos (administrativos, personal) o incluso para su transporte (ordenanzas) está obligado a preservar la confidencialidad sobre los datos del paciente y por tanto a guardar secreto profesional de la información a la que puedan acceder.

RECOMENDACIÓN

Sería recomendable que todos los hospitales establecieran normas internas que obliguen a la confidencialidad de los datos, tanto al personal del hospital como a todo aquel que pueda tener acceso datos de los pacientes, como médicos residentes, estudiantes o personal externo.

Todo el personal citado debería suscribir un compromiso de confidencialidad antes de empezar a desempeñar sus funciones mediante el cual se acepte la norma interna descrita.

B. CONCLUSIÓN

En algunos hospitales se ha implantado un sistema de turno para las consultas basado en el uso de tickets anonimizados, de tal forma que cuando se llama a un paciente que está en la sala de espera se utiliza el código asignado en el ticket y no su nombre y apellidos, preservando su identidad al resto de pacientes. No obstante, se ha comprobado que no se usa este sistema en todos los casos, de modo que cuando el paciente no acude a la llamada por el código asignado se le llama por megafonía utilizando su nombre y apellidos.

En algunos casos el sistema de tickets anonimizado es utilizado o no a criterio del facultativo que llama al paciente.

Si bien no se han encontrado listas de pacientes citados en las zonas de consultas, en diversos hospitales han tenido que prohibir esta práctica por ser habitual entre algunos facultativos.

RECOMENDACIÓN

Se recomienda utilizar los sistemas de turno para las consultas que preserven el anonimato de los pacientes cuando son llamados. Un buen sistema es el de tickets anonimizados siempre que se encuentren instalados, no dejando a criterio del facultativo su utilización.

No se debe fijar la lista de los pacientes citados en las zonas de consultas.

4.4.5. CONCLUSIÓN art.15, 16, 17 LOPD – Derechos ARCO

En todos los centros inspeccionados las solicitudes de acceso de los pacientes a su HC se centralizan en el Servicio de Atención al Paciente, salvo en algún caso que son evaluadas además por el departamento jurídico.

Cuando se solicita acceso a la HC, con carácter general el servicio de Atención al Paciente pregunta qué documentación es la que le interesa, ya que en la mayoría de las ocasiones es para solicitar una segunda opinión sobre un proceso médico y únicamente necesita un subconjunto de la HC.

Se ha encontrado que siempre se pide documento de identificación del afectado, así como una autorización escrita y un documento acreditativo de identificación de la persona que lo recoge, en su caso. En el caso de menores se solicita la acreditación del padre, madre o tutor legal, con presentación del libro de familia.

La copia de la HC se entrega generalmente en un CD, para facilitar las imágenes médicas junto con los informes, o bien en papel. Esta documentación se entrega en mano o se envía por medio de correo certificado con acuse de recibo.

En uno de los centros auditados se ha solicitado al interesado abonar los gastos del correo certificado, en contra de lo especificado en el artículo 4.2 del RDLOPD: “Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición”. En otro centro distinto se encontró que inicialmente repercutían al paciente el coste de las copias de las imágenes médicas, si bien en el momento de la inspección habían establecido ya un procedimiento gratuito.

Los facultativos de los centros que disponen de HC automatizada, suelen marcar las anotaciones subjetivas como información no imprimible de tal forma que no se replica cuando se realiza la copia. Además esta información subjetiva suele estar accesible únicamente al personal médico que la ha generado.

RECOMENDACIÓN

El derecho de acceso debe concederse mediante un procedimiento sencillo y gratuito para el paciente. En caso de que el envío se realice por correo certificado con coste para el paciente, se deberá ofrecer un medio gratuito, como por ejemplo recoger la

documentación personalmente en el propio centro. Lo anterior no será de aplicación en aquellas Comunidades Autónomas que han desarrollado legislación que habilita el cobro de una tasa al ejercitar el derecho de acceso.

Al paciente se le deberá permitir optar por la modalidad por la que se le facilita la documentación solicitada en su ejercicio de acceso.

Los derechos de rectificación y cancelación estarán sujetos a las limitaciones establecidas en la LAP.

4.4.6. CONCLUSIÓN - Oposición a facilitar datos

Algunos centros han establecido grupos de trabajo para analizar el procedimiento a implementar para atender el posible requerimiento de un paciente de que no se facilite su número de habitación en caso de hospitalización a familiares que pregunten telefónicamente o de forma presencial.

Se ha detectado confusión y preocupación en los hospitales a la hora de determinar en qué situaciones se puede dar información a una persona que acuda al hospital a preguntar por un paciente, y qué información se puede facilitar.

RECOMENDACIÓN

Se debe establecer un procedimiento para recabar el consentimiento del paciente con relación a si desea o no que sea facilitada información sobre su presencia y ubicación en el hospital a personas o familiares que pregunten por ello en la ventanilla de información del hospital. Siempre y cuando el paciente no se haya opuesto a que dicha información sea facilitada, considerando que pudieran existir situaciones de urgencia vital y que la presencia de familiares o allegados pudiera ser esencial para la debida atención del paciente, el hospital puede informar si la persona se encuentra en urgencias o se encuentra ingresada y el número de habitación, sin indicar datos de salud o la atención médica prestada.

4.4.7. CONCLUSIÓN art.12 LOPD y art 88.5 RDLOPD - Prestación de servicios

El artículo 12 de la LOPD regula las cláusulas que deben contemplarse en los contratos de prestación de servicios que impliquen tratamiento de datos de carácter personal.

Entre los hospitales objeto de esta inspección sectorial se han detectado algunos casos en los que no se ha podido evidenciar el establecimiento de un acuerdo de encargado del tratamiento con las empresas que prestan servicios externos y que tratan datos de salud de los pacientes. En otros casos estos acuerdos de encargados de tratamiento constan en los pliegos de cláusulas administrativas o técnicas de los pliegos de contratación, si bien en algunos casos no se encuentran completas.

Asimismo se ha detectado que, en algunos casos, en el documento de seguridad no consta la identificación de los ficheros sobre los que un encargado externo realiza

tratamientos ni una referencia al contrato ni la identidad del encargado de tratamiento o periodo de vigencia del contrato.

RECOMENDACIÓN

En la documentación contractual de las prestaciones de servicios con acceso a datos personales debe estipularse el encargo del tratamiento de acuerdo a lo previsto en el artículo 12 de la LOPD: *"la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, debiéndose establecer en el expresamente que:*

- *el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento,*
- *no los aplicará o utilizará con fin distinto al que figure en dicho contrato,*
- *ni los comunicará, ni siquiera para su conservación, a otras personas."*

En el contrato se estipularán además las medidas de seguridad, estando el encargado del tratamiento obligado a implementarlas.

Se debe exigir asimismo que, una vez cumplida la prestación contractual, los datos de carácter personal sean destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

Debe incorporarse en los Documentos de Seguridad una referencia expresa al contrato de encargado del tratamiento firmado con la entidad pertinente, así como el periodo de vigencia del mismo.

Al mismo tiempo, sería recomendable comenzar a incluir en los nuevos contratos las cláusulas que el Reglamento General de Protección de Datos (RGPD) considera necesarias. Esta Agencia ha elaborado unas directrices a este respecto.

Por otro lado, los contratos de prestación de servicios firmados con anterioridad a la aplicación del RGPD en mayo de 2018 deben modificarse y adaptarse para respetar este contenido.

MEDIDAS DE SEGURIDAD

Las inspecciones, realizadas con la normativa en vigor en 2016, han vuelto a arrojar, al igual que ocurrió en el anterior plan sectorial, múltiples deficiencias con relación a las medidas de seguridad. El enfoque de la seguridad de los Sistemas de Información va a sufrir un cambio con la aplicación del nuevo RGPD en mayo de 2018. Las medidas de seguridad que relacionan a continuación son de obligado cumplimiento en la actualidad, y constituyen un punto de partida para su adaptación, en función de los resultados de los análisis de riesgo y de las Evaluaciones de Impacto que se van a tener que realizar, a las exigencias de seguridad previstas en el RGPD.

4.4.8. CONCLUSIÓN art. 89 RDLOPD - Funciones y obligaciones del personal

En algunos hospitales se ha comprobado que, como medida informativa adicional, se muestra un aviso de confidencialidad al iniciar la aplicación de acceso a la HC, informando al trabajador de que sólo debe acceder a los datos si es necesario para su desempeño profesional, que todos los accesos quedan registrados, que está prohibida su difusión o comunicación a terceros, y que el incumplimiento de las normas puede generar la adopción de medidas legales.

En otros hospitales existe un aviso similar al iniciar el ordenador, en vez de la aplicación que maneja la HC.

También se ha encontrado un aviso más sencillo que informa de la confidencialidad de los datos a los que se accede, del registro de los accesos y de la necesidad de cerrar la aplicación al terminar.

RECOMENDACIÓN

Debido a la especial naturaleza de los datos de salud tratados en los hospitales, se recomienda la adopción de avisos de confidencialidad al iniciar las aplicaciones que tienen acceso a los datos personales, resumiendo estos aspectos:

- que sólo debe acceder a los datos si es necesario para su desempeño profesional,
- que todos los accesos a los datos de los pacientes quedan registrados,
- que está prohibida la difusión de los datos personales y su comunicación a terceros,
- que no se deben realizar copias de datos médicos de los pacientes fuera de los ficheros y soportes establecidos por el centro y
- que el incumplimiento de estas normas puede generar la adopción de medidas legales contra el trabajador

En los centros que trabajan mayoritariamente con la HC en formato papel debería incorporarse en la carátula de la HC las recomendaciones indicadas anteriormente aplicables a documentación en papel así como la responsabilidad de custodia y protección de la información para evitar su pérdida o el acceso por terceros.

4.4.9. CONCLUSIÓN art. 90 y 100 RDLOPD – Registro de incidencias

En los centros inspeccionados se ha constatado que no se ha implantado un procedimiento de gestión de incidencias como tal, limitándose en la mayoría de los casos a tramitarlas por medio de los centros de atención al usuario. Además, en los procesos de recuperación, en algunos casos, no se registran ni documentan casos derivados de la pérdida de documentos en papel que necesitan ser recuperados.

En varios hospitales se ha verificado que el registro de incidencias es común para todos los ficheros con datos personales. Los usuarios que detectan una incidencia deben comunicarla al Departamento de Informática por correo electrónico o por

teléfono. Estas incidencias se registran en una aplicación CAU (Centro de Atención al Usuario) y se procede a su gestión.

Se ha detectado que algunos hospitales que conservan parte de la HC en papel −si bien disponen de un registro de incidencias relacionadas con el transporte de documentos, historias no localizadas, incidentes con la empresa que las gestiona, etc.− no se ha podido evidenciar la existencia de un procedimiento escrito para la notificación y registro de incidencias de documentos en papel. El registro de incidencias no se extiende a todos los documentos que puedan contener datos de carácter personal, sino que es aplicable únicamente a las HC.

Se ha acreditado que en uno de los centros la referencia que figura en el Documento de Seguridad relativa a la gestión de las incidencias no se adecúa a la realidad (hace referencia a que las incidencias se registran en una aplicación que en realidad es un gestor documental que no se utiliza para este fin).

En otro de los centros se ha detectado que el registro no refleja en todos los casos las incidencias que son resueltas, por lo que pueden no constar aspectos relacionados con la recuperación de datos de carácter personal.

Para todos los hospitales que tienen aplicaciones departamentales independientes del área de Informática, las incidencias se resuelven localmente o por medio de las empresas externas que administran la aplicación, quedando estas fuera del registro de incidencias, sin que conste la autorización del responsable del fichero.

RECOMENDACIÓN

Debe definirse e implantarse un procedimiento para la notificación y registro de incidencias en lo referente a los documentos en soporte papel. Podría optarse por aprovechar el sistema de registro de incidencias establecido para ficheros automatizados, añadiendo un campo para poder diferenciar las relacionadas con el soporte papel de las del informático.

El procedimiento a desarrollar para la notificación y registro de incidencias relacionadas con los ficheros no automatizados debe contemplar las actividades a llevar a cabo para la recuperación de la información en caso de pérdida de los soportes.

Además de contemplar todas las incidencias ocurridas en la entidad, en el caso de que para resolverlas sea necesario hacer una recuperación de datos, se debe registrar la autorización por parte del responsable, así como las actividades llevadas a cabo para la misma.

El documento de seguridad deberá contener un detalle del procedimiento de gestión y control de incidencias ocurridas con ficheros de datos de carácter personal.

4.4.10. CONCLUSIÓN art. 91 RDLOPD - Control de Acceso. Alertas

Se ha comprobado que algunas de las aplicaciones revisadas, que facilitan acceso a datos de salud a los facultativos, levantan alertas si el facultativo que realiza la

consulta accede a datos de un paciente que no tiene asignado, debiendo justificar el acceso. Sin embargo, la mayoría de las aplicaciones auditadas permiten que un facultativo acceda a datos de pacientes que no tiene asignados.

Algunas aplicaciones permiten también definir alertas que se disparan cuando un paciente ha solicitado confidencialidad de sus datos por una condición especial, tal como la existencia de una orden de alejamiento por violencia de género.

RECOMENDACIÓN

Los profesionales asistenciales que realizan el diagnóstico o el tratamiento del paciente deben poder acceder a la historia clínica atendiendo a lo estipulado en el art. 16 de la LAP.

No obstante, se recomienda que, siempre que sea factible atendiendo a criterios de prestación de la asistencia sanitaria (en consultas externas más factible que en urgencias), el sistema de información o las aplicaciones que faciliten el acceso a los datos de los pacientes eleven alertas visibles al usuario para aquellos casos en los que el usuario acceda a los datos de un paciente que no tiene asignado o que no le corresponde en principio atender, estableciéndose un tratamiento especial del registro del acceso que incluya la justificación del mismo.

Se recomienda el establecimiento de otras alertas de confidencialidad que se muestren al usuario del sistema cuando acceda a los datos de un paciente concreto que ha solicitado una especial protección.

A este respecto debe destacarse que los accesos injustificados a las HC por parte de los profesionales sanitarios pueden dar lugar a la exigencia de responsabilidades disciplinarias por parte de la Administración en la que preste servicios el profesional. Asimismo, el Código Penal recoge el delito de revelación de secretos, también aplicable a estos accesos injustificados y la utilización posterior de la información accedida, condenado incluso con penas de cárcel.

4.4.11. CONCLUSIÓN art. 91 RDLOPD - Control de Acceso. Perfiles. Gestión de usuarios

En todas las aplicaciones que gestionan la HC electrónica existen diferentes perfiles de acceso, limitándose la información clínica que puede ser visualizada. Esto mismo ocurre en algunas aplicaciones departamentales, si bien la mayoría de ellas, generalmente con pocos usuarios, no limitan adecuadamente el acceso a la información para algunos perfiles.

En algunas aplicaciones corporativas se ha comprobado que algunos colectivos o perfiles de usuarios tienen acceso a datos que no necesitan para sus funciones, tales como, por ejemplo, los administrativos de admisión de hospitalización que tienen acceso a alertas que no les son relevantes (por ejemplo, las alertas de infecciosos son relevantes para hospitalización pero alertas de alergias al látex no, que sin embargo sí son relevantes para listas de espera de cirugía, tratadas por otro departamento). Se ha detectado también que en determinadas aplicaciones personal administrativo puede tener acceso a informes médicos, no siendo necesario para sus funciones.

RECOMENDACIÓN

Cada usuario del Sistema de Información debe tener acceso a la información del paciente mínima necesaria para realizar sus funciones, pudiéndose implementar esta limitación en base a perfiles de acceso más restrictivos, sobre todo en el caso del personal no sanitario que realiza tareas administrativas, al que se debe limitar el acceso a los datos de HC relacionados con sus propias funciones de acuerdo con el art. 16.4 de la LAP.

4.4.12. CONCLUSIÓN art. 91 RDLOPD - Control de Acceso. Gestión de Perfiles.

En la mayoría de los centros hay instaladas aplicaciones departamentales en las que la gestión de los usuarios, incluidas altas, bajas y asignación de perfiles, se realiza por el responsable del departamento o, en muchas ocasiones, por una entidad externa encargada del mantenimiento de la aplicación.

RECOMENDACIÓN

En el documento de seguridad debe figurar el personal autorizado para conceder, alterar o anular los accesos autorizados sobre los datos de los pacientes, conforme a criterios establecidos el responsable del fichero. Además, en caso de tratarse de una entidad externa, en el contrato de prestación de servicios debe constar expresamente la encomienda de la gestión de usuarios y privilegios.

4.4.13. CONCLUSIÓN art.93 RDLOPD - Identificación y Autenticación. Cambio de contraseñas

Se ha encontrado un número significativo de aplicaciones que no exigen el cambio de contraseña en el primer inicio de sesión, no asegurándose así la confidencialidad de la misma en el momento de su distribución. En unos casos, los identificadores de usuario y contraseñas de acceso se entregan en papel al usuario, en otros se comunican verbalmente, o se envían por correo electrónico. En un centro se asigna siempre una contraseña por defecto a todos los usuarios, que el sistema no fuerza a modificar en el primer acceso.

Para varias de las aplicaciones auditadas, incluidas algunas de las que dan acceso a la HC de los pacientes, no se ha establecido un plazo de caducidad de las contraseñas de los usuarios.

RECOMENDACIÓN

Se debe establecer una política de cambio de contraseñas que garantice que el periodo de vigencia sea inferior a un año.

El procedimiento de asignación y distribución de las contraseñas deberá garantizar su confidencialidad, considerándose una buena práctica para los casos en que terceros intervengan en este procedimiento, ya sea el caso de distribución en papel, por correo

electrónico, teléfono, contraseñas iniciales preestablecidas, etc., que las aplicaciones obliguen al usuario al cambio de contraseña en el primer acceso.

4.4.14. CONCLUSIÓN art.93 RDLOPD - Identificación y Autenticación

Se ha verificado que una de las herramientas web que permiten visualizar en el navegador datos de salud no cierra correctamente la sesión, manteniendo los datos del último paciente accedido hasta que se cierra el navegador. De este modo, se permite el acceso latente a algunos datos de salud sin necesidad de autenticar al usuario.

RECOMENDACIÓN

Se debe solicitar la autenticación del usuario siempre que se cierre la sesión o que el usuario lleve un tiempo sin actividad.

4.4.15. CONCLUSIÓN art.93 RDLOPD - Identificación y autenticación. Usuarios genéricos

Se ha detectado que en algunos hospitales se utilizan usuarios genéricos para el acceso a determinados sistemas de información, tales como ordenadores que controlan equipamiento de laboratorio, terminales de monitorización (por ejemplo, en el paritorio) o ecógrafos.

Algunos equipos, como los ecógrafos, almacenan directamente datos personales. En otros sistemas los datos personales se encuentran disociados con un código: en el laboratorio de análisis clínicos todos los datos de las analíticas se encuentran identificados en los equipos únicamente por un código de muestra y, si bien este código corresponde a un paciente, en los ordenadores de laboratorio que utilizan usuarios genéricos no se puede resolver la disociación y averiguar a qué paciente corresponde.

En algunos casos se ha argumentado que se utilizan estos usuarios genéricos por necesidades del servicio ligada a los cambios de guardia y la necesidad de mantener una continuidad en la utilización de los equipos médicos.

En un hospital se han encontrado códigos de usuarios genéricos y sus contraseñas publicadas en guías internas de fin de semana para servicios generales si bien los representantes del hospital han manifestado que estos usuarios ya no se utilizan y se han eliminado.

En varios hospitales se han encontrado pegatinas adheridas a los ordenadores con los códigos de los usuarios genéricos y sus contraseñas escritas en ellas, situación que equivale a la eliminación de la utilización de códigos de usuario como control de acceso. Incluso en algún caso se ha constatado que desde el ordenador que tiene la pegatina se puede acceder a la aplicación principal de gestión de la HC, si bien al iniciar esta aplicación se procede a realizar la autenticación del usuario.

Existen algunas aplicaciones que tratan datos de salud que utilizan arquitecturas cliente-servidor con muy pocos usuarios, basando su seguridad en la necesidad de tener instalado un módulo cliente en el puesto de trabajo, y no disponiendo de código de usuario ni contraseña.

RECOMENDACIÓN

Debe establecerse un mecanismo que permita la identificación inequívoca y personalizada de los usuarios que acceden a datos personales, verificando el sistema que el usuario se encuentra autorizado y registrando la actividad del mismo.

No se deben utilizar usuarios genéricos para tratar datos personales.

En los casos en los que los datos de salud se encuentren disociados de los datos identificativos por medio de un código sí se podrían utilizar sistemas genéricos de autenticación de usuario aunque, se recomienda evitar su utilización

La asignación, distribución y almacenamiento de contraseñas debe realizarse de forma segura, siendo cada usuario responsable de la custodia de su contraseña. En ningún caso deben escribirse las contraseñas en lugares visibles tales como los puestos de trabajo.

En ningún caso es suficiente como medida de control de acceso la necesidad de tener instalado un módulo cliente para acceder a los datos personales, debiendo implementarse mecanismos de autenticación inequívoca y personalizada.

4.4.16. CONCLUSIÓN art.93 RDLOPD- Identificación y autenticación. Almacenamiento de la contraseña

En una de las aplicaciones corporativas utilizadas para la gestión de los datos de los pacientes, incluidos datos de salud tales como informes de alta y diagnóstico, se ha verificado que el personal de informática con los privilegios adecuados puede visualizar las contraseñas de los usuarios de la aplicación. Esta facilidad se utiliza para suministrar la contraseña a los usuarios cuando estos la olvidan.

RECOMENDACIÓN

Las contraseñas de los usuarios deberán almacenarse de forma ininteligible.

En el caso de olvido de la contraseña por parte del usuario, se debe distribuir de forma segura una nueva contraseña que se recomienda que se fuerce su cambio en la primera sesión.

4.4.17. CONCLUSIÓN art.98 RDLOPD - Identificación y Autenticación. Limitación accesos reiterados.

No todas las aplicaciones auditadas bloquean a un usuario tras un número de intentos de acceso fallidos.

RECOMENDACIÓN

Se deben de establecer mecanismos que limiten la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Los intentos repetidos de acceso con una contraseña errónea deben dar lugar al bloqueo del usuario.

4.4.18. CONCLUSIÓN art. 94, 102 RDLOPD - Copia de seguridad

Con carácter general se realizan copias de respaldo diarias de la información almacenada en los sistemas de información centralizados de todos los centros inspeccionados. No obstante, se han encontrado varias referencias escritas donde se indica que las copias se realizan con una periodicidad al menos semanal. Sin embargo, los representantes del hospital han manifestado que de la mayoría de los sistemas, incluidos los que soportan la HC, la copia de seguridad se realiza de forma diaria.

No todos los hospitales auditados disponen de una copia completa en segunda ubicación de todos los datos de nivel alto. Sólo una parte de la información se envía a través de la red del Servicio de Salud de la Comunidad Autónoma correspondiente a una segunda ubicación.

En determinados hospitales se realizan pruebas de restauración de un muestreo de ficheros semanalmente y diariamente se revisan los *logs* de las copias y el sistema de copias realiza una prueba de restauración de la copia. Aunque las pruebas del software no se realizan con los datos reales (es decir, los existentes en el entorno de producción), se utiliza una copia de los mismos que no se ha anonimizado, por lo que podrían darse accesos a información, sin la aplicación de las medidas de seguridad previstas reglamentariamente.

En otro hospital se automatiza determinada información como los informes de alta, y además tiene instaladas aplicaciones departamentales y corporativas que residen en su CPD, y dispone de un sistema de ficheros que trabaja de modo redundante en clúster, lo que implica que mantienen copias de los datos de forma continua, aunque en la misma ubicación. Además de lo anterior, se realizan copias de seguridad diariamente sobre toda la información, que se remite a un centro físicamente apartado y se genera un informe para los responsables de informática sobre la inexistencia de errores.

Varias veces al año se hacen pruebas de restauración de algún fichero para verificar la corrección del proceso. Sobre estos ficheros restaurados que contienen datos reales de pacientes se prueban parches del sistema operativo o del sistema de gestión de bases de datos o actualizaciones de la aplicación.

Estos sistemas de prueba no se ponen en explotación y no se da acceso a personal del hospital.

Hay aplicaciones sobre las cuales se realizó una prueba de restauración aproximadamente siete meses antes de la inspección realizada, mientras que para

otras aplicaciones no hay previsto ningún protocolo de prueba de restauración. Se ha verificado sobre la máquina que se realizan las restauraciones que en la última de ellas se había producido un error que continuaba sin solucionarse.

En otro de los hospitales visitados la realización de las copias de seguridad de las aplicaciones departamentales recae sobre el departamento en cuestión, desconociendo el departamento de informática si se realizan copias de respaldo y sus procedimientos.

RECOMENDACIÓN

Se deben realizar copias de respaldo para todas las aplicaciones que mantienen datos de salud, como mínimo semanalmente, debiendo mantenerse las copias en una ubicación distinta junto con los procedimientos de recuperación correspondientes.

Se recomienda establecer un plan de continuidad y recuperación ante desastres eficaz, que puede jugar un importante papel en la marcha y supervivencia de cualquier organización. Es además una poderosa herramienta para mantener a los hospitales preparados ante incidentes graves.

Cada seis meses se deben de realizar verificaciones sobre el correcto funcionamiento y aplicación pruebas de restauración de los procedimientos de la realización de copias de respaldo y recuperación. Se recomienda revisar el estado de los discos que funcionan en clúster para evitar las pérdidas de información que se podrían producir en caso de que se vayan encadenando fallos en diferentes discos.

Si es necesario utilizar los datos restaurados para la realización de pruebas, deben garantizarse las mismas medidas de seguridad que los que se encuentran en explotación y deberán ser físicamente destruidos cuando finalicen las pruebas.

Se debe detallar en el documento de seguridad el procedimiento de eliminación de los ficheros generados en las pruebas de restauración. En ningún caso utilizar ficheros temporales con datos reales para pruebas o desarrollos.

Deben anonimizarse los datos utilizados para la realización de pruebas del software desarrollado (bien por personal propio o por terceros). En caso contrario deben aplicarse las mismas medidas de seguridad exigidas para el entorno de producción (copia de seguridad, registro de accesos, revisión del registro de accesos, gestión de altas de usuario y de contraseñas, etc.)

4.4.19. CONCLUSIÓN art. 96, 110 RDLOPD – Auditoría de seguridad

Se ha detectado en la mayoría de los hospitales que el plazo máximo de dos años para la realización de auditorías de las medidas de seguridad sobre todos los ficheros es superado, realizándose en todo caso auditorías parciales en una selección de ficheros.

En algunos documentos de seguridad se refleja la realización de auditorías bienales, pero se realizan de forma parcial sobre una selección de ficheros de los centros hospitalarios.

En dos de los hospitales, la razón alegada para la no realización de la auditoría es encontrarse a la espera de entrar en la auditoría planificada por la Consejería de Sanidad de la Comunidad Autónoma correspondiente, detectándose por tanto un problema de asignación y definición de las tareas y las responsabilidades que conlleva la no realización de acciones obligatorias.

Se han encontrado medidas correctoras en los informes de auditoría que no se han llegado a aplicar.

RECOMENDACIÓN

Al menos cada dos años se deben realizan auditorías internas o externas que verifiquen el cumplimiento de las medidas de seguridad sobre todos los ficheros que contengan datos personales.

Para realizar la auditoría de todos los ficheros en los plazos legales, ésta podría abordarse de manera progresiva, auditando los distintos ficheros en distintos momentos del año, pero siempre sin que se superen los dos años.

Debería revisarse la relación de tareas de auditoría previstas y extenderla tanto a los tratamientos centralizados en los centros de proceso de datos de los hospitales como a los distribuidos o departamentales que, en ocasiones, son administrados por terceras entidades y no consta que se realice control alguno sobre éstos.

Las deficiencias identificadas en las auditorías deben subsanarse aplicando las medidas correctoras adecuadas.

4.4.20. CONCLUSIÓN art. 104 RDLOPD - Comunicaciones cifradas

Se ha detectado que, si bien la mayoría de las comunicaciones electrónicas de datos de salud en entornos hospitalarios se realizan por redes privadas cifradas, en algunos casos específicos tales como durante los trámites de derivaciones de pacientes entre hospitales, informes de alta de urgencias remitidos a los juzgados, intercambio de información con centros de atención primaria o el envío de hojas de asistencia desde Admisión, se remite documentación con datos de salud a través de redes públicas de telecomunicaciones sin cifrado (vía fax).

También se han detectado casos en los que el envío de datos de salud se realiza por correo electrónico, como el caso del envío de informes de resultados desde los servicios a los centros de salud.

Algunos hospitales disponen de una red WiFi para el acceso a diversas aplicaciones en los portátiles de las plantas. Aunque se trata de redes WiFi con filtrado por dirección IP y MAC, el cifrado utilizado en algunos casos es WEP que no ofrece unas mínimas garantías de seguridad, ya que un usuario malintencionado podría romper la contraseña WEP fácilmente y descifrar el tráfico capturado.

RECOMENDACIÓN

Todas las comunicaciones de datos de salud que se realicen a través de redes públicas de telecomunicaciones se efectuarán cifrando dichos datos o utilizando otro

mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. No está por tanto permitida la remisión de datos de salud vía fax sin cifrado.

Si fuese estrictamente necesario utilizarlo, deben aplicarse procesos de disociación de los datos con anterioridad al envío por redes públicas.

Igualmente, debería cifrarse el contenido del correo electrónico en caso de envío de datos de nivel alto.

Debe modificarse el sistema de cifrado utilizado para la red WiFi, de manera que éste se encuentre acorde con el estado de la tecnología, (en la actualidad se recomienda que sea al menos WAP2 con una contraseña de cifrado robusta).

4.4.21. CONCLUSIÓN art. 113 RDLOPD - Control de acceso a la HC en soporte papel para fines asistenciales

No se ha acreditado que los hospitales que utilizan la HC en papel dispongan de una relación de personas autorizadas para acceder a la información en soporte papel.

RECOMENDACIÓN

Debe elaborarse una relación de personal autorizado a acceder a la documentación en soporte papel de cada servicio, que incluya el perfil de acceso.

4.4.22. CONCLUSIÓN art. 114 RDLOPD - Traslado de documentación de HC en soporte papel

Se ha identificado que en algunos casos en que es necesario trasladar al paciente en ambulancia para la realización de pruebas, la HC es trasladada con el propio paciente por el técnico de la ambulancia, quien podría acceder a la información al no haberse dispuesto medidas de seguridad para evitar accesos no autorizados.

En este mismo centro el traslado de los resultados de los análisis realizados por el departamento de Anatomía Patológica se envía a las plantas del hospital en sobres abiertos.

En uno de los hospitales se ha verificado que el transporte de estas historias se realiza en carros tapados con lonas lo que impide en cierta medida el acceso a la documentación. En otro hospital los carros son abiertos. Además, en ambos casos los carros no pueden ser introducidos en la consulta por su tamaño, por lo que durante algunos instantes las HC se quedan en zonas de acceso al público sin custodia. No obstante, con carácter general se dan instrucciones a los encargados del reparto para que transporten únicamente un carro y que tengan especial cautela con la custodia de las HC.

En otro de los hospitales visitados, que aún utiliza HC en papel, el reparto de HC se realiza de tal forma que los documentos pueden quedar desatendidos en los departamentos que en los que se entregan. Se pudo comprobar que en un servicio de especialidad, que se encontraba con la puerta abierta y sin personal, las HC se

hallaban depositadas en estanterías al alcance de la mano. La existencia de un cartel que solicitaba “¡POR FAVOR! PONER LAS HISTORIAS DEL DÍA SOBRE LA MESA. (GRACIAS)” da a entender que lo habitual es que el departamento en cuestión se encuentra desatendido cuando se distribuyen las HC.

RECOMENDACIÓN

Es necesario implementar procedimientos que permitan controlar el acceso de documentos con datos médicos, designándose un grupo de personas responsables de su gestión.

Deben implantarse medidas para el traslado de las HC tales como sobres cerrados con procedimiento de notificación y de recepción por parte de los centros de destino para verificar que la historia no ha sido accedida ni modificada durante el traslado. Otra posibilidad sería que la HC fuese trasladada por personal específico que se encargue de su custodia ininterrumpida.

En este sentido, deben establecerse medidas para que en ningún momento se pierda la cadena de custodia por parte del personal que traslada las historias clínicas. Esto puede conseguirse de diferentes formas: dedicando dos personas para el reparto, introduciendo el carro en las consultas para las entregas o bien utilizando carros cerrados que no planteen dudas sobre la custodia de las historias.

Sería recomendable también colocar un formulario en cada historia que permita identificar, al menos, al solicitante, fecha de recogida, fecha de devolución y motivo o justificación del acceso. También se podría desarrollar una aplicación informática para el registro de estos eventos.

4.4.23. CONCLUSIÓN art. 92, 97 101 RDLOPD - Gestión de soportes automatizados

No todos los hospitales inspeccionados han realizado un inventario de soportes que contengan datos de carácter personal. Se ha comprobado que en diversos centros existen ordenadores personales, portátiles y tabletas que no están inventariados, si bien no se permite a los usuarios que almacenen en estos equipos datos personales.

En otros centros se comprobado que se mantienen soportes informáticos con datos de nivel alto que no se encuentran inventariados. Por ejemplo, soportes CD de radiología que se distribuyen a otros servicios. No se limita ni controla el uso de soportes USB, pudiendo los usuarios utilizar este tipo de soportes USB para fines personales.

Aunque los representantes del hospital entienden que no se producen entradas y salidas de soportes informáticos, esta situación impide la aplicación de las medidas de seguridad sobre protección de soportes, previstas en los artículos 92, 97 y 101 en cuanto al etiquetado, inventariado, registro de entrada y de salida y cifrado de los mismos.

RECOMENDACIÓN

Identificar correctamente los soportes con datos de salud especialmente los dispositivos portátiles.

Asimismo, se deben cifrar los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

Evitar el uso de soportes USB, bloqueando su uso en los equipos donde no sea necesario para las funciones encomendadas al usuario.

4.4.24. CONCLUSIÓN art. 92, 108 RDLOPD - Gestión y custodia de HC en soporte papel

Se ha detectado que el sistema de HC en papel conlleva dificultades inherentes, tales como el problema de comprobación de:

- la conservación de la integridad del contenido,
- si se han realizado copias de los documentos,
- si se ha extraído la HC o parte de su contenido fuera del hospital antes de devolverla,
- si se ha enseñado a terceros.

Una vez repartida la HC a los diversos departamentos para su uso, su custodia queda totalmente en manos de los profesionales que la tienen en préstamo, no existiendo con carácter general normas internas escritas con instrucciones de la utilización de las HC en papel y, como se ha indicado, se han evidenciado situaciones de almacenamiento temporal de HC de forma desatendida en servicios de especialidad con la puerta abierta.

Además se han encontrado casos en los que la documentación de la HC no se conserva en archivadores dotados de cerradura, o si bien disponían de llave ésta se encontraba puesta, incluso en salas que se encuentran siempre abiertas: en un archivo temporal de Anatomía Patológica los resultados de informes se conservaban en archivadores tipo AZ en estanterías sin cierre, en una sala que permanece siempre abierta; en un Laboratorio de Hematología no todos los informes de análisis se encuentran almacenados en estanterías bajo llave; en un archivo de un servicio de especialidad se archivan informes con datos de nivel alto en archivadores AZ que no disponen de cierre.

En algunos casos las HC en papel incluyen un inventario con la documentación que contienen. También se han encontrado sistemas de etiquetado con pegatinas que incluyen códigos de expediente, y números secuenciales para las carpetas que contienen las HC.

Todos los centros inspeccionados disponen de contenedores de papel destinados a la destrucción confidencial por medio de una tercera entidad contratada al efecto, o de destructoras de papel.

RECOMENDACIÓN

Se deben establecer mecanismos de comprobación de la integridad de la HC en papel, tal como la numeración de cada una de las páginas que se añaden, incluyendo y actualizando un índice de documentos contenidos, e informando en los préstamos las normas a seguir en el manejo de la HC y las responsabilidades en las que se puede incurrir en caso de no observar las mismas.

Además, se debe incluir en las funciones y obligaciones del personal con acceso a la HC en papel información relativa a la prohibición del copiado de datos médicos, de la exposición a terceros, y de la salida de la documentación fuera del recinto, además de normas sobre la custodia y protección de la HC.

Debe realizarse un análisis de la capacidad de almacenar de forma segura documentación con datos de salud en todos los servicios de los centros hospitalarios y, en caso de deficiencias, dotarlos de archivadores que permitan a los usuarios almacenar la documentación con datos de carácter personal bajo llave. Además deben establecerse procedimientos para la gestión de las llaves de manera que estas no se queden en las cerraduras.

Los archivos, como corresponde a datos con medidas de seguridad de nivel alto, deben encontrarse en salas cerradas.

4.4.25. CONCLUSIÓN art. 103 RDLOPD - Registro de accesos

En la mayoría de los hospitales se ha evidenciado que determinados departamentos utilizan documentos ofimáticos para almacenar, de forma temporal o permanente, datos de salud de los pacientes. Dependiendo del hospital estos documentos se almacenan en carpetas de red ubicadas en el CPD o localmente en algún ordenador personal ubicado en el propio departamento. Según se ha comprobado, en ninguno de los dos casos se han habilitado mecanismos para el registro de los accesos sobre estos ficheros. Además, los documentos ofimáticos que se encuentran en ordenadores personales se encuentran fuera de la política de copias de seguridad del hospital.

No todas las aplicaciones disponen de registro de accesos y las que lo tienen tampoco disponen, en todos los casos, de un periodo definido de conservación.

También se han detectado registros de acceso que sólo almacenan información relativa al usuario que se conecta, la fecha y la hora, pero no qué actuaciones concretas se han realizado sobre un determinado registro o paciente.

En algunos centros no se realizan auditorías con la información que consta en los registros de acceso, tan sólo a demanda de las autoridades judiciales o administrativas, o en caso de incidentes.

RECOMENDACIÓN

Deben adecuarse los sistemas de registro de acceso en las aplicaciones que no lo han implementado o que se encuentran incompletas. Para cada intento de acceso se debe almacenar la siguiente información: identificación del usuario, fecha y hora, fichero al

que se ha accedido, tipo de acceso y si ha sido autorizado o denegado. En caso de que haya sido autorizado será preciso guardar la información que permita identificar el registro al que se ha accedido. Los registros de acceso deberán almacenarse por un periodo mínimo de dos años.

Debe evitarse la utilización de carpetas locales o en red para el almacenamiento de documentos ofimáticos con datos de nivel alto, ya que no es posible disponer para estos casos del registro de accesos de acuerdo a los términos previstos, pudiéndose quedar el fichero fuera de las políticas de seguridad del centro. Debería implantarse un gestor documental para estos casos, que permita habilitar estos registros de auditoría así como el resto de medidas de seguridad aplicables.

Deben revisarse, al menos mensualmente, los registros de accesos, elaborando un informe que determine los puntos revisados y los resultados de las revisiones. Para facilitar el tratamiento de los registros de accesos, podrían desarrollarse procedimientos de explotación automáticos (tales como scripts) que permitan obtener informes de actividad con los parámetros previamente definidos.

4.4.26. CONCLUSIÓN art. 108 RDLOPD - Custodia de documentación en papel

Se ha comprobado que en los mostradores de algunos puestos de enfermería de planta de algunos de los hospitales visitados se encuentran documentos con datos de los pacientes hospitalizados, a la vista de las personas o pacientes que se acercan al puesto.

En otro hospital figura, en el informe de auditoría, que como norma general no se aplican las políticas de mesas despejadas, habiéndose identificado en los distintos servicios visitados documentación sobre las mesas, sin aparente custodia por parte de personal autorizado, así como que en el despacho de admisión de urgencias se distribuyen las historias a devolver por encima de mesas, sin ser recogidas cuando no hay personal.

RECOMENDACIÓN

Los mostradores de atención al paciente, en los puestos de enfermería y en cualquier otro lugar con presencia de público, las mesas y mostradores deben de estar limpios de documentos que contengan datos personales.

Debe formarse y concienciar a todo el personal sobre la necesidad de aplicar este tipo de políticas, así como dotar de infraestructura que permita la protección de la documentación hasta su archivo definitivo.

RECOMENDACIONES GLOBALES SOBRE APLICACIONES DEPARTAMENTALES NO INTEGRADAS DENTRO DEL SISTEMA DE INFORMACIÓN CORPORATIVO

CONCLUSIÓN. Islas de información departamentales

En algunos hospitales se ha detectado un número significativo de aplicaciones, e incluso equipos informáticos, instalados sin conocimiento del departamento de informática, o aplicaciones de las cuales este departamento no ha tenido conocimiento hasta la ocurrencia de alguna incidencia con relación a los mismos. Se han detectado asimismo situaciones en las cuales, aun conociendo el departamento de informática la existencia de las aplicaciones, desconocía las medidas de seguridad implementadas o no sobre estas aplicaciones, incluida la autenticación de usuarios y registro de accesos.

Se ha evidenciado, además, la duplicación, en algunos casos, de los sistemas de información: en algunos servicios coexiste la estructura de los sistemas de información sanitaria generales, que a veces se considera por parte de los empleados incompleta o con lagunas de información, con sistemas paralelos organizados por cada departamento, normalmente más cercanos a las necesidades diarias, pero con carencias importantes en medidas seguridad y en ocasiones fuera de la normativa interna del hospital.

Por ejemplo, en uno de los hospitales auditados los facultativos piden directamente datos a farmacia sobre dispensaciones a pacientes, manteniendo el departamento de farmacia su propia aplicación con más datos de los incluidos en el Sistema de Información Corporativo del Hospital. En otro hospital, el laboratorio tiene su propio Sistema de Información que no borra ningún dato aunque la información se trasfiere al Sistema Corporativo que gestiona las historias clínicas, alegando que los datos no se pueden explotar tan eficientemente como en el Sistema Corporativo.

Esta duplicación de datos puede derivar además en inconsistencias de la información almacenada, si se produce una modificación en los datos de uno de los sistemas que no se traslada al otro.

RECOMENDACIÓN

Cualquier equipo o aplicación informática debe ser instalada, gestionada y supervisada por el departamento de informática o por cualquier otro designado por el responsable del fichero, que deberá verificar que cumple con las medidas de seguridad y las políticas de protección de datos establecidas por el hospital. Deben establecerse normas internas en este sentido, asegurándose de que son conocidas por todo el personal del hospital.

En caso de duplicación de sistemas, además de lo anterior, se deberá de implementar un proceso que garantice la consistencia y la calidad de la información.

5. DESCRIPCIÓN DEL MODELO DE GESTIÓN DE DATOS EN EL ÁMBITO DE LA INVESTIGACIÓN MÉDICA

5.1. INFORMACIÓN RECABADA DE LOS RESPONSABLES DE REALIZAR INVESTIGACIÓN MÉDICA EN LOS CENTROS AUDITADOS

De las entrevistas realizadas en los hospitales auditados con los diversos actores que participan en proyectos de investigación médica se desprende lo siguiente:

En los centros hospitalarios se realizan esencialmente dos tipos de investigación:

- Investigación básica, que fundamentalmente persigue un mejor conocimiento de los mecanismos biológicos implicados en los procesos salud-enfermedad sin la búsqueda de su aplicación práctica, por lo que se realiza sin acceso a datos personales de pacientes, y no es objeto de este informe.

- Investigación clínica, cuyo objetivo principal es la mejora del diagnóstico, tratamiento y prevención de enfermedades en humanos, para lo cual en ocasiones es necesario el acceso a los datos de los pacientes. Dentro de la investigación clínica se encuentran, entre otros:
    - ensayos clínicos, normalmente con medicamentos, aunque también incluyen otro tipo de actuaciones con prótesis, técnicas quirúrgicas, etc. Estos ensayos conllevan tratamientos de datos de salud de los sujetos objeto del estudio, tanto sanos como enfermos.
    - estudios retrospectivos, tesis, proyectos de fin de grado, etc., que pueden conllevar el acceso a la HC de pacientes.

Si bien en la mayoría de las investigaciones llevadas a cabo los sujetos son pacientes del hospital, en algunos casos no es así, ya que también se realizan investigaciones con voluntarios sanos. En estos casos, los estudios realizados a los sujetos suelen incluir una pequeña HC, realizada específicamente para el estudio, que no se integra en el archivo de HC del hospital.

Como toda investigación científica la investigación médica es un proceso sistemático y organizado. Es sistemático porque aplica el método científico y sigue ordenadamente todos sus pasos. Y es organizado porque los distintos investigadores emplean en todo momento criterios y procedimientos estandarizados, dentro de una metodología predefinida en el protocolo del estudio. Por ello, todo investigador que quiere realizar una investigación, si quiere que ésta sea válida y reconocida, debe someterse a un protocolo que no puede ignorar. Este protocolo contempla, entre otros aspectos, los tratamientos que se deben realizar con datos de los sujetos participantes. Toda investigación que quiera ser reconocida no puede contemplar la realización de accesos indiscriminados a datos personales fuera del protocolo aprobado.

Los grandes hospitales tienen un CEIm, Comité Ético de Investigación médica, (antes CEIC) que es independiente en sus funciones, y que vela entre otros aspectos por la protección de los derechos y seguridad de los sujetos participantes en proyectos de investigación clínica, emitiendo para ello un dictamen sobre:

- El protocolo del estudio, que incluye el objetivo, consideraciones éticas, de confidencialidad y protección de datos, etc.
- Los métodos y los documentos que vayan a utilizarse para informar a los sujetos del ensayo, como la Hoja de Información al Paciente (HIP) que incluye información sobre protección de datos y que suele ser entregada junto con el consentimiento informado (CI).
- Otras cuestiones como la idoneidad de los investigadores, la adecuación de las instalaciones, el contrato de seguro, etc.

Asimismo, el CEIm debe informar, a petición del promotor, investigadores u organismos de financiación, cualquier estudio de investigación en materia sanitaria que implique la participación directa de seres humanos o en el que se utilicen muestras de origen humano, o datos personales, incluidos estudios observacionales, tesis y proyectos de fin de grado, siendo siempre aplicables, en cualquier caso, las recomendaciones internacionales tales como la Declaración de Helsinki, promulgada por la Asociación Médica Mundial en junio de 1964, o el Convenio Europeo sobre los Derechos Humanos y la Biomedicina, de abril de 1997 (Convenio de Oviedo).

Es posible que un hospital (con pocos proyectos de investigación) no tenga CEIm, canalizando en este caso sus iniciativas de investigación a través del departamento de asesoría jurídica, y para el caso de los ensayos clínicos se deben adherir a ensayos multicentro que ya han pasado los controles de los CEIm's de otros centros que participan en el ensayo, y que han sido autorizados por la Agencia Española del Medicamento y Productos Sanitarios.

Es también posible que un CEIm de un hospital actúe como CEIm de referencia y tutele los ensayos clínicos de otros hospitales que carecen de CEIm. El hospital también puede constituir una Comisión de Investigación, que autoriza los estudios retrospectivos, tesis y proyectos de investigación y controla que cumplan con los criterios de calidad exigibles.

Ensayos clínicos

Tienen generalmente como objetivo la evaluación experimental de un medicamento, aunque también pueden evaluar una determinada terapia sin medicamentos, un producto, o una técnica diagnóstica, y se encuentran regulados por el RD-ECM.

En los centros hospitalarios inspeccionados se ha comprobado en la documentación asociada a diversos ensayos clínicos que tienen definida las siguientes figuras, de forma resumida:

- **Un Investigador Principal (IP):** es la figura del profesional médico del hospital responsable de la investigación.

- **Un promotor**: responsable de iniciar, gestionar y organizar la financiación de un ensayo clínico, en su mayoría empresas farmacéuticas.

  La propiedad de los datos de la investigación pertenece al promotor desde el primer momento del estudio, si bien no tiene acceso a los datos de identificación de los sujetos participantes en el ensayo. Según manifestaciones de los representantes de los centros inspeccionados, la recogida de datos y las

comunicaciones de resultados de la investigación se mantienen en repositorios de datos disociados (sin identificación del paciente).

- **Un contrato:** suscrito por el promotor, el investigador principal, y la dirección del hospital. En caso de existir fundación de investigación, ésta también lo suscribe.
- **Un protocolo:** documento donde se describen los objetivos, el diseño, la metodología, las consideraciones estadísticas y la organización de un ensayo clínico. Comprende las sucesivas versiones de los protocolos y sus modificaciones, que en caso de producirse deben de ser validadas de nuevo.
- **Consentimiento Informado (CI)** prestado por parte de los sujetos del ensayo, que refleja la expresión libre y voluntaria de su voluntad de participar en un ensayo clínico determinado, tras haber sido informados de todos los aspectos del mismo que sean pertinentes para su decisión de participar. Estos CI se recogen en formato papel y los custodia bajo llave el investigador principal o su equipo de apoyo. También, se entrega al paciente una **HIP** (Hoja de Información al Paciente) que incluye información sobre Protección de Datos.
- **Cuaderno de recogida de datos (CRD):** cada ensayo tiene su sistema de recogida de datos, facilitado por el promotor. El responsable del tratamiento del CRD es el promotor. No obstante, los datos facilitados por el equipo de investigación del hospital al promotor no incluyen la identificación del paciente.
- **Póliza de seguro:** por las posibles responsabilidades en caso de daños producidos.

El IP y su equipo de investigadores, si así ha sido autorizado, son los únicos que conocen los datos identificativos de los participantes en un ensayo clínico, siendo estos datos desconocidos para el promotor, en virtud de la disociación de datos realizada.

El IP tiene la capacidad de revertir la disociación a través del código que se asigna a cada paciente en el marco del ensayo. El proceso de revertir la disociación de datos se realiza de forma excepcional, tan solo cuando es necesario, entre otras razones, por la seguridad del participante ante posibles efectos adversos que se puedan producir durante el ensayo, para prestarle la atención médica que necesita. En ningún caso se revierte la disociación para facilitar datos personales al promotor.

En la HC del Sistema de Información del hospital se incluye, para cada paciente que participa en un ensayo clínico, toda información sobre el ensayo practicado, ya que puede ser de especial relevancia para la atención sanitaria del paciente. A esta HC sólo tiene acceso el personal sanitario autorizado por el hospital.

Además, en el marco de cada ensayo clínico se mantiene un fichero de HC propio, distinto de la HC del hospital, con la información relevante para cada paciente, tal como las analíticas que se realizan a los sujetos como consecuencia de su participación en el ensayo. Esta HC propia constituye la documentación manejada en el ámbito del ensayo clínico, y a la que se tiene acceso por parte de auditores como el monitor para la comprobación de la corrección de los datos facilitados en el CDR, evitando así el acceso a la HC no anonimizadas del hospital.

La tabla que recoge los códigos de participantes asociados a los datos identificativos del paciente puede ser un documento en papel, o puede estar automatizada en un fichero ofimático normalmente del tipo Excel o Access.

5.2. CÓDIGO TIPO DE FARMAINDUSTRIA

La Asociación Nacional Empresarial de la Industria Farmacéutica establecida en España (Farmaindustria) ha desarrollado un código tipo de protección de datos personales en el ámbito de la Investigación Clínica y Farmacológica que ofrece a los laboratorios que voluntariamente se adhieran al mismo una uniformidad en la aplicación de medidas de protección de datos de carácter personal.

Estas medidas afectan a los centros hospitalarios auditados ya que en la totalidad de ellos se realizan investigaciones médicas cuyos promotores son los laboratorios adheridos a Farmaindustria, estableciendo el siguiente modo de actuación:

Fase previa a la investigación clínica

Todo ensayo clínico comienza con la redacción de un Protocolo por parte del Promotor.

El Monitor, profesional cualificado elegido por el Promotor que tiene encomendado el seguimiento directo de la investigación, actúa como vínculo entre el Promotor e Investigador y se encarga en esta fase de verificar la idoneidad del centro donde se va a realizar la investigación (en el ámbito de estas actuaciones de oficio: el hospital) y del investigador.

El Comité Ético de Investigación Médica estudia el protocolo y valora, entre otros condicionantes, la protección de los derechos, seguridad y bienestar de los sujetos que participan en el ensayo. Uno de los requisitos para que la investigación pueda realizarse es contar con un informe favorable del CEIm.

Recogida de datos personales de los sujetos

Una vez aprobado el proyecto de investigación, el Investigador y su equipo seleccionan los sujetos que participarán en el estudio conforme a los criterios establecidos en el Protocolo. Para ello acceden a la documentación que figura en la HC de los hospitales auditados.

Desarrollo de la investigación clínica

La investigación clínica se realiza tratando datos personales, que posteriormente se disocian para incorporarlos en el CRD.

El procedimiento de disociación de datos debe ser irreversible de modo que a todo personal ajeno al Investigador y su equipo suponga un esfuerzo desproporcionado asociar nuevamente los datos de la investigación con la identidad de los sujetos participantes.

Durante el desarrollo de la investigación clínica, el Investigador llevará a cabo las actuaciones establecidas en el Protocolo, registrando los datos disociados en el fichero Cuaderno de Recogida de Datos.

El Promotor no accederá en ningún momento a datos de carácter personal de los sujetos participantes en el ensayo ni participará en la recogida de datos. La comunicación entre el Promotor e Investigador se realiza por medio del Monitor.

No obstante, el promotor recibirá del Investigador copia de los CRD que no incluyen datos personales de los participantes.

El Monitor, por su lado, debe verificar la exactitud e integridad de la información que figura en el CRD, teniendo acceso a la HC del sujeto, que contiene datos identificativos junto a información médica, limitándose a la visualización de esta información, no estando habilitado a recogerlos ni registrarlos.

Todo ensayo clínico puede tener un auditor que tendrá acceso a los datos personales de los sujetos con la finalidad de prestar el servicio de auditoría limitándose a su visualización no estando habilitado a recogerlos ni registrarlos.

La gestión de las reacciones adversas es realizada por el IP, para lo cual debe revertir la disociación de datos. Asimismo, la gestión de las coberturas de los seguros debe realizarse por el IP, quien tendrá que comunicar los siniestros a la entidad aseguradora. De esta forma, aunque el seguro es contratado por el promotor, éste no tiene acceso a los datos personales que se facilitan a las compañías de seguros.

El responsable del tratamiento de los datos personales de los participantes es el hospital, siendo el Investigador Principal el responsable del ensayo, y el encargado de custodiar la tabla que permite revertir la disociación de los datos de los participantes.

Finalización del estudio

El Promotor recibe del Investigador información y conclusiones desprovistas de datos personales, por lo que éste a su vez podrá comunicarlos libremente a terceros y no estará obligado a aplicar medidas de seguridad.

La documentación generada deberá permanecer en el hospital, concretamente los formularios de consentimiento informado firmados, originales de la HC del sujeto, lista de códigos de identificación utilizada para la disociación de los datos en el CRD.

5.3. COMPROBACIONES REALIZADAS EN LAS ACTUACIONES DE INSPECCIÓN

En las actuaciones presenciales realizadas en el ámbito de este plan sectorial se ha verificado que en los hospitales inspeccionados se realiza investigación clínica/epidemiológica con acceso a datos de pacientes. Este tipo de investigación incluye tanto estudios observacionales como ensayos clínicos con o sin medicamentos.

En los ensayos clínicos a que se ha tenido acceso se ha comprobado que los sujetos participan de forma voluntaria y que han suscrito previamente un consentimiento informado.

Se ha comprobado que los CEIm son independientes de otras áreas y departamentos de los centros hospitalarios y que emiten dictámenes que permiten iniciar o no una investigación cuando ésta trata datos personales de pacientes. Los ensayos clínicos son evaluados en cuanto a sus aspectos metodológicos, éticos y legales, emitiendo un dictamen. También mantiene un inventario de los ensayos en curso, teniendo registrada la documentación asociada, que incluye entre otros documentos el contrato, su protocolo, modelo de cuaderno de recogida de datos, hoja de información al paciente y consentimiento informado, póliza de seguro, etc.

Para el cometido de sus funciones el CEIm no tiene acceso a los datos identificativos de los sujetos del estudio.

Ensayos clínicos

Un ensayo clínico puede referirse tanto al estudio de un medicamento como al de una técnica terapéutica o diagnóstica (sin utilización de medicamentos).

Antes de la realización del ensayo clínico, toda la documentación previa es evaluada por el CEIm, y una vez aceptada, se exige la conformidad del gerente del hospital y la firma de un contrato.

Son el IP (Investigador Principal) y su equipo de investigadores los responsables de facilitar al sujeto la información sobre el ensayo, incluyendo la HIP (Hoja de Información al Paciente) y el CI (Consentimiento Informado), llevándose el sujeto los documentos a su domicilio para estudiarlos y poder consultar su posible participación en el ensayo con su familia.

Una vez firmado el CI se guarda, custodiado por el IP, seguidamente se solicita un código aleatorizado que facilita el promotor y se comienza a introducir sus datos (disociados mediante el código) en el CRD.

Cada ensayo tiene su cuaderno de recogida de datos (CRD), en papel o mediante un sistema o programa informático, habitualmente facilitado por el promotor. El responsable del tratamiento del CRD en los ensayos clínicos con medicamentos es el promotor, tal y como se recoge en el código tipo de la industria farmacéutica. El promotor no tiene acceso en ningún caso los datos personales de los sujetos, ya que siempre se introducen en el CRD disociados.

Se ha comprobado que el Investigador Principal (IP) y su equipo de investigadores son los únicos que conocen los datos identificativos de los participantes en un ensayo clínico. Para el resto de los participantes en el ensayo los datos se encuentran disociados. Sólo el IP o algún miembro de su equipo en el que haya delegado es el único que tiene la capacidad de revertir la disociación y acceder a la identificación del sujeto.

En algunas ocasiones el IP es el promotor del ensayo. No obstante, siempre se sigue el procedimiento descrito de disociación.

Otras investigaciones, estudios observacionales

Todo investigador que desea realizar un proyecto debe diseñarlo y presentarlo al CEIm para su evaluación, debiendo este diseño contener al menos los siguientes elementos: protocolo, HIP y CI, memoria económica, compromiso del IP y otros documentos que pueden ser específicos según el proyecto.

Para los estudios observacionales con medicamentos, una vez evaluados por el CEIm, se exige la conformidad de la Consejería de Salud de la Comunidad Autónoma y la firma de un contrato.

Para las investigaciones dentro del marco de una tesis, un proyecto fin de grado o una ponencia para la cual se deba acceder a HC se exige también la firma de un contrato.

En todos los estudios se exige la obtención del CI del sujeto participante, salvo que se justifique que es un esfuerzo desproporcionado y sea aceptado por el CEIm. Estos casos se refieren a estudios retrospectivos observacionales o revisiones de HC, y para recibir autorización debe garantizarse que no se van a publicar datos personales, especificándolo así en el proyecto.

No obstante lo anterior, dada la facilidad detectada para el acceso a las historias clínicas de todos los pacientes por parte del personal médico autorizado, es posible que facultativos de un hospital accedan a HC para realizar estudios e investigaciones que no son evaluadas por el CEIm. Para evitarlo se realizan labores formativas, tanto a los estudiantes de medicina como a los facultativos del hospital para que conozcan claramente en qué tipo de estudios e investigaciones es necesario elaborar un proyecto y solicitar el informe favorable previo del CEIm.

Se ha verificado que los datos personales de los sujetos objeto de la investigación o ensayo clínico no se tratan para fines distintos de la propia investigación o asistencia sanitaria.

En algunos casos excepcionales, como cuando el estudio conlleva traslados de los sujetos participantes con coste al proyecto, se hace necesario tratar los datos con dicha finalidad. El procedimiento utilizado es comunicar los datos únicamente a la agencia de viajes que va a gestionar el traslado, sin comunicarlos al promotor, aunque sea éste el que se haga cargo de los gastos. En estos casos se pide a los sujetos el consentimiento para el tratamiento de sus datos con dicha finalidad.

5.4. CONCLUSIONES Y RECOMENDACIONES SOBRE LOS TRATAMIENTOS DE DATOS REALIZADOS CON LA FINALIDAD DE INVESTIGACIÓN

5.4.1. CONCLUSIÓN. Consentimiento para el acceso a datos con la finalidad de realizar estudios de investigación retrospectivos, tesis o publicaciones por parte de facultativos o departamentos del hospital

Si bien los facultativos o departamentos no suelen realizar investigaciones por su propia cuenta sin someterlas a la aprobación de un CEIm o Comisión de Investigación (entre otros motivos han manifestado que no resulta productivo realizar investigaciones que luego no puedan ser reconocidas o publicadas), se ha encontrado que los facultativos pueden acceder a las HC para revisión retrospectiva de los casos de forma particular, sin el marco de una investigación auditada por el CEIm o una Comisión.

En los estudios en los que interviene un CEIm o Comisión se exige la obtención del CI del sujeto participante, exceptuándose en aquellos casos en los que resulte un esfuerzo desproporcionado, normalmente en estudios retrospectivos o revisiones de HC, siempre y cuando no se vayan a publicar datos personales, y teniendo en cuenta que por lo general los únicos datos personales relevantes de los pacientes en estos estudios son la edad y el sexo, sin interesar su nombre y apellidos u otros datos identificativos.

Se han encontrado hospitales en los que no está definido que intervenga un CEIm o Comisión para cada uno de los estudios que realizan los facultativos, no solicitándose con carácter general el consentimiento a los pacientes para el tratamiento de sus datos médicos con finalidad de investigación retrospectiva, elaboración de tesis o publicaciones.

RECOMENDACIÓN

Se debe informar, y solicitar el consentimiento de los pacientes, con relación a la posible utilización de sus datos de salud para la finalidad de realizar estudios de investigación retrospectivos, tesis o publicaciones.

En caso de que lo anterior resulte imposible o se considere un esfuerzo desproporcionado, se deberán establecer mecanismos que aseguren que los accesos con fines de investigación se realicen asegurando el anonimato de los pacientes, preservando los datos identificativos del paciente separados de los clínicos, como se indica en el art.16.3 de la LAP.

5.4.2. CONCLUSIÓN. Registro y control del acceso a la HC para estudios de investigación retrospectivos, tesis o publicaciones

En los centros que disponen de HC en papel, o parcialmente automatizada, normalmente se establecen procedimientos para el control del acceso a las historias

clínicas físicas mediante unos formularios en los que se identifica al investigador, al departamento y el motivo del acceso.

Se ha evidenciado, tras examinar estos formularios, que los motivos de acceso consignados son muy vagos (tales como “estudio” o “revisión”) convirtiéndose el procedimiento en un mero trámite sin auditar y concediéndose el acceso en todos los casos, resultando que la única finalidad del procedimiento es la de registrar los accesos. Estas peticiones de HC suelen ser sin mediación de CEIm o Comité, ya que no se desarrollan en el marco de un ensayo clínico y habitualmente se accede a esta documentación para escribir un artículo médico o para realizar ponencias en congresos.

También, se han encontrado centros con la HC automatizada (total o parcialmente) en los que el personal médico tiene potencial acceso, sin restricción, a las historias clínicas de todos los pacientes, los tenga asignados o no, por lo que pueden acceder con fines de investigación.

RECOMENDACIÓN

Es necesario implementar procedimientos que permitan controlar el acceso a documentos con datos médicos para otros fines distintos a los asistenciales, designándose un grupo de personas responsables de su gestión. Debe restringirse el acceso ilimitado a las historias clínicas de aquellos pacientes que no estén asociados a cada facultativo o al menos a cada departamento, independientemente que estas se encuentren automatizadas o no.

Para facilitar una HC en papel a un determinado facultativo debería consultarse en una aplicación informática si el paciente está asignado o no.

Debe registrarse el solicitante, la fecha de recogida, la fecha de devolución y el motivo o justificación del acceso. También se podría desarrollar una aplicación informática para el registro de estos eventos.

Asimismo se debería realizar un listado con los motivos autorizados para acceder a una determinada HC para realizar estudios retrospectivos y auditar periódicamente los accesos para verificar que se realizan conforme a la normativa.

5.4.3. CONCLUSIÓN. Salas de lectura de HC para investigación

En varios hospitales se han encontrado habilitadas salas de lectura de documentación clínica, para la consulta de HC en papel por parte del personal facultativo.

En uno de los hospitales se utiliza una sala de lectura con taquillas cerradas donde se guardan las HC solicitadas, pudiendo el personal médico, con su tarjeta de empleado, abrir exclusivamente la taquilla que contiene las HC que él ha solicitado. No obstante, en el momento de realizar la inspección se observó que en el suelo de la sala había un conjunto de historias clínicas fuera de las taquillas, al alcance de la mano.

Para el acceso a la sala se utiliza igualmente la tarjeta de empleado, estando restringido al personal médico solicitante y empleados del archivo.

En otro hospital se ha encontrado un procedimiento escrito en el que se detalla que solo tienen acceso a las HC para su estudio el personal sanitario cualificado del Hospital. En este hospital la consulta de la HC se realiza en una sala ubicada en el Archivo Central.

RECOMENDACIÓN

Las salas habilitadas para el acceso a las historias clínicas deben incluir medidas de seguridad física para garantizar que sólo el solicitante de una determinada documentación tiene acceso a la misma.

Además se recomienda realizar revisiones periódicas para verificar el funcionamiento de estas salas y que la documentación se almacena correctamente, no quedando sin control a disposición de terceros. Se debe prestar especial atención a los procesos de entrega y retirada de la documentación ya que se ha detectado que son los momentos de mayor exposición.

5.4.4. CONCLUSIÓN. Identificación de sujetos en ensayos clínicos

Se ha encontrado que la tabla que permite revertir la disociación (que contiene los códigos de los participantes asociados a los datos identificativos del paciente), ya sea en papel, o fichero informático, se encuentra siempre custodiada personalmente por el IP o su equipo de trabajo, no estando en ocasiones incluida dentro del circuito de medidas de seguridad del centro.

En algunos casos, la tabla de identificación de los sujetos se encuentra marcada como confidencial.

RECOMENDACIÓN

La tabla que permite revertir la disociación, ya se encuentre en papel o en un fichero informático, debe estar sujeta a las políticas de seguridad del centro, de tal forma que le sean aplicadas las medidas de seguridad como a cualquier otro fichero con datos personales.

Por la especial relevancia de esta tabla de identificación de los sujetos, se considera una buena práctica marcarla como confidencial e incluir una leyenda informativa de la necesidad de mantener su carácter confidencial.

5.4.5. CONCLUSIÓN. Contratos ensayos clínicos

Algunos contratos de ensayos clínicos estipulan la obligación del Investigador Principal o de su equipo de informar verbalmente al paciente, entregarle la Hoja de Información y recoger su CI. Otros no recogen expresamente esta obligación, si bien se encuentra recogida en la normativa y es exigida por el CEIm. Todos hacen referencia general al cumplimiento de la LOPD o a normativa de protección de datos en general.

No se especifican expresamente en el contrato aspectos importantes como:

- la prohibición de tratar los datos personales de los sujetos para otras finalidades,

- qué ocurre con los datos al acabar el ensayo,
- las medidas de seguridad aplicables,
- la obligación de que en las publicaciones de los resultados deba mantenerse la anonimización de los datos.

Con carácter general se incluye en el contrato el compromiso por parte del IP de la custodia de los códigos de identificación de pacientes y de la disociación de los datos personales de los sujetos para que no puedan ser identificables por el promotor.

Los contratos incluyen compromiso de confidencialidad de los datos personales por todas las partes intervinientes, si bien se han encontrado modelos de contratos que en su redacción exceptúa el compromiso de confidencialidad sobre aquella información *"que fuera conocida previamente por el investigador principal o por el Hospital en el momento de ser revelada*", lo cual no constituye una excepción válida.

RECOMENDACIÓN

Sería recomendable que en el contrato se incluyera la prohibición de tratar los datos personales de los sujetos para otras finalidades distintas a la investigación. Asimismo sería recomendable especificar qué ocurre con los datos al acabar el ensayo, las medidas de seguridad a aplicar a los datos, y la anonimización de los datos necesaria en las publicaciones de los resultados.

El compromiso de confidencialidad debe abarcar sin excepciones toda información que contenga datos personales de los sujetos participantes.

5.4.6. CONCLUSIÓN. Información sobre protección de datos en ensayos clínicos

La información estipulada por el art. 5 de la LOPD se ha encontrado sólo en algunas ocasiones incluida en los CI examinados. Con carácter general se hace mención a la confidencialidad de los datos pero no se mencionan los derechos ARCO. Tampoco se menciona la identidad y dirección del responsable del tratamiento, máxime cuando en el CI aparecen la figuras del IP, el promotor, el hospital y en ocasiones otras instituciones como el CNIO.

Se han encontrado consentimientos informados con información confusa con respecto a los tratamientos, refiriéndose, por ejemplo, expresamente a datos de salud asociados a datos identificativos, y a que el personal del estudio estará autorizado a revelar esa información a diferentes actores, entre ellos el promotor. Sin embargo, posteriormente, en el cuerpo del documento se indica que los datos comunicados al promotor son "codificados". También se han encontrado imprecisiones como que se mantendrá la confidencialidad de los datos "siempre que no sean imprescindibles para el desarrollo del proyecto".

RECOMENDACIÓN

La información sobre el tratamiento de datos personales facilitada a los sujetos del ensayo debe ser lo más clara posible y sin ambigüedad. Esta información debe incluir

lo estipulado en el art. 5 de la LOPD, considerándose una buena práctica el incorporarla en el documento de Consentimiento Informado o en la Hoja de Información al Paciente.

Deberá informarse del procedimiento a seguir para el ejercicio de los derechos ARCO, haciendo mención expresa de la entidad a la que dirigirse o del representante designado, y su dirección.

Deberá informarse asimismo de las consecuencias especiales de la salida voluntaria del sujeto del ensayo clínico (al revocar su consentimiento) y, en su caso, que los datos recogidos hasta la fecha serán conservados para no desvirtuar la investigación, si bien no se tratarán ni recogerán más datos después de la retirada del consentimiento.

Por último, se deberá informar al sujeto sobre la publicación de los resultados de la investigación. En caso de que no sea posible la publicación sin datos identificativos del sujeto, éstos solo podrán ser publicados cuando haya mediado el consentimiento previo y expreso del sujeto.

5.4.7. CONCLUSIÓN. Finalización de ensayos clínicos

Al finalizar el ensayo clínico es el IP, como responsable del ensayo, el encargado de la custodia de los datos personales (incluyendo los datos identificativos de los sujetos participantes y los CI) y el Promotor, el responsable de los Cuadernos de Recogida de Datos (con datos sin identificación, disociados). En algunos centros, es práctica habitual que el IP, una vez que el ensayo está totalmente finalizado, envíe al Archivo del hospital toda documentación relativa al ensayo para su custodia.

RECOMENDACIÓN

Los hospitales, como responsables del tratamiento, deben implementar protocolos que establezcan los mecanismos de custodia de los datos personales una vez finalizados los ensayos clínicos.

5.4.8. CONCLUSIÓN. Tratamientos con otras finalidades en las investigaciones

No se han encontrado tratamientos de datos para otras finalidades distintas a la asistencial y la investigación, tales como finalidades publicitarias.

La única finalidad distinta encontrada ha sido cuando el estudio conlleva traslados de los sujetos participantes con coste al proyecto, siendo el procedimiento comunicar los datos únicamente a la agencia de viajes que va a gestionar el traslado, sin comunicarlos al promotor, aunque sea éste el que se haga cargo de los gastos. Además, en estos casos se pide a los sujetos el consentimiento para el tratamiento de sus datos con dicha finalidad.

RECOMENDACIÓN

Cuando se haga necesario tratar los datos de los sujetos participantes con otras finalidades distintas a la investigación o la asistencial, deberá solicitarse su consentimiento.

5.4.9. CONCLUSIÓN. Tratamientos de datos de salud de personas sanas

En las investigaciones con sujetos sanos (que no son pacientes del hospital) se han encontrado Historias Clínicas realizadas específicamente para el estudio que no se integran en el archivo de HC general del hospital, almacenándose en papel bajo la responsabilidad del Investigador Principal.

RECOMENDACIÓN

Todos los datos personales de los sujetos participantes, ya se encuentren en papel o en un fichero informático, deben estar sujetos a las políticas de seguridad del centro, de tal forma que les sean aplicadas las medidas de seguridad como a cualquier otro fichero con datos personales.

6. NUEVOS REQUERIMIENTOS REGULADOS EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Dentro de las medidas de responsabilidad activa exigidas por el RGPD, que entrará en vigor en mayo de 2018, se encuentran las Evaluaciones de Impacto, cuyo concepto se introduce en su artículo 35.

Su realización es obligatoria de forma previa a la puesta en marcha de nuevos tratamientos que entrañen un alto riesgo. No obstante, en relación a los tratamientos ya preexistentes en los hospitales actualmente en funcionamiento, esta Agencia considera que, a partir de mayo de 2018, a medida que se vayan incorporando nuevos datos de pacientes, y en la medida que son tratamientos a gran escala de datos de categorías especiales, sí será necesario llevar a cabo una Evaluación de Impacto, por lo que se debería de ir planificando su ejecución.

Una Evaluación de Impacto es un proceso que mide la necesidad y proporcionalidad de un determinado tratamiento de datos así como los riesgos que implica para los derechos y libertades de las personas físicas. Permite demostrar a los responsables de los ficheros que se han adoptado las medidas adecuadas para cumplir con la nueva normativa de protección de datos.

Para realizar estas evaluaciones, los hospitales deberán disponer de un registro de tratamientos de datos personales de los que son responsables, incluyendo la finalidad, las categorías de datos implicados y los perfiles de usuario autorizados a realizar cada tratamiento. También se deberá realizar una evaluación de los riesgos a que está sometidos los tratamientos, el impacto que cada riesgo tendría en los derechos y libertades de los pacientes y una descripción de las medidas de seguridad técnicas y organizativas adoptadas.

El proceso iterativo para la realización de la evaluación de impacto tendrá, al menos, las siguientes fases:

1. Descripción de los tratamientos de datos de los pacientes previstos.
2. Evaluación de la necesidad y proporcionalidad.
3. Medidas de seguridad previstas para cumplir con la normativa.
4. Evaluación de los riesgos para los derechos y libertades de los pacientes.

5. Medidas a implementar para reducir los riesgos.
6. Elaboración de la documentación.
7. Monitorización del estado de implementación de las medidas de seguridad y repaso de los riesgos a que se ven sometidos los datos de los pacientes y repetición continua del proceso desde el punto 1.

Las Evaluaciones de Impacto deberán ser actualizadas a lo largo del ciclo de vida de cada tratamiento, teniendo en cuenta los nuevos riesgos y las variaciones en el impacto. Por tanto, puede ser necesario repetir procesos de evaluación ya que la adopción de nuevas medidas técnicas u organizativas puede afectar a los riesgos a que se ven sometidos los tratamientos. La realización de la Evaluación de Impacto es un proceso continuo, no se realiza en un único ciclo.

La Evaluación de Impacto debe realizarla el centro hospitalario responsable del tratamiento, que es por tanto el responsable de su elaboración, aunque debe contar con el asesoramiento del Delegado de Protección de Datos, una figura que también recoge el Reglamento Europeo. Las decisiones adoptadas deberán ser parte de la documentación de la Evaluación de Impacto. Además si el tratamiento de datos es realizado total o parcialmente por una tercera entidad, ésta debe proporcionar la información necesaria al hospital. Si la decisión final del responsable del tratamiento difiere de la del encargado del tratamiento, deberá documentarse el motivo por el que se realiza o no el tratamiento de datos de salud.

Hay señalar que la incorporación de un Delegado de Protección de Datos es obligatoria para los responsables o encargados que cuenten, entre sus actividades principales, los tratamientos a gran escala de datos sensibles, así como para las Administraciones públicas, entre otros supuestos, por lo que los Hospitales Públicos deberán contar con dicha figura a partir de mayo de 2018. El Delegado de Protección de Datos deberá tener autonomía en el ejercicio de sus funciones, las cuales podrá desarrollar a tiempo total o parcial, en este último caso, siempre y cuando no surjan conflictos de intereses: el Delegado de Protección de Datos no podrá supervisar tareas que sean fruto de su propio trabajo.

7. CONCLUSIONES FINALES

Este informe representa un paso más en la tarea iniciada por la AEPD en 1995 cuando por primera vez se abordó con carácter general un análisis sobre el grado de aplicación de la normativa de protección de datos en el sistema sanitario.

El contenido del presente informe pone de manifiesto la tendencia en general favorable a la progresiva asunción, no solo de la normativa, sino de los principios y la cultura sobre la relevancia del tratamiento de los datos en este sector y su debida protección. Con todo aún se deben y se pueden mejorar, entre otros aspectos, los relacionados con:

- la calidad y la confidencialidad de los datos conservados,
- la información ofrecida a los pacientes así como a los sujetos participantes en los ensayos clínicos,
- la obtención de los consentimientos en todos los casos en que este sea necesario,
- y el reforzamiento de las medidas de seguridad, potenciando con carácter general los mecanismos de control de acceso.

Por otro lado, con el diagnóstico que se deriva de este informe, la AEPD pretende ofrecer un punto de referencia con el que todos los integrantes del sector sanitario puedan abordar la adaptación de sus sistemas y procedimientos a los nuevos requerimientos que impone el Reglamento Europeo, de plena aplicación a partir del 25 de mayo de 2018.

En este sentido, y como ya se ha apuntado anteriormente, la profundización en la cultura, la formación y los principios que informan sobre la trascendencia de los tratamientos de los datos personales en este sector resulta un elemento capital en el que habrá que seguir profundizando y que, por lo que al personal sanitario y administrativo del sector se refiere, bien podrían resumirse en los diez principios o decálogo que se presenta a continuación:

1. Trata los datos de los pacientes como querrías que tratasen los tuyos.
2. ¿Estás seguro de que tienes que acceder a esa historia clínica? Piénsalo. Sólo debes hacerlo si es necesario para los fines de tu trabajo.
3. Recuerda: tus accesos a la documentación clínica quedan registrados en el sistema. Se sabe en qué momento y a qué información has accedido. Los accesos son auditados posteriormente.
4. Evita informar a terceros sobre la salud de tus pacientes salvo que estos lo hayan consentido o tengas una justificación lícita.
5. Cuando salgas del despacho, asegúrate de cerrar la sesión abierta en tu ordenador. No facilites a nadie tu clave y contraseña; si necesitas un acceso urgente contacta con el servicio de informática.
6. No envíes información con datos de salud por correo electrónico o por cualquier red pública o inalámbrica de comunicación electrónica; si tienes que hacerlo, no olvides cifrar los datos.
7. No tires documentos con datos personales a la papelera; destrúyelos tú mismo o sigue el procedimiento implantado en tu centro.
8. Cuando termines de pasar consulta, cierra con llave los armarios o archivadores que contengan documentación clínica.
9. No dejes las historias clínicas a la vista sin supervisión.
10. No crees por tu cuenta ficheros con datos personales de pacientes; consulta siempre antes con el departamento de informática.

Listado de siglas

AEMPS	Agencia Española de Medicamentos y Productos Sanitarios
CEIm	Comité Ético de Investigación Médica
CI	Consentimiento informado
CIP	Código de Identificación Personal
CIPA	Código de Identificación Personal Autonómico
CNIO	Centro Nacional de Investigaciones Oncológicas
CRD	Cuaderno de Recogida de Datos de un Ensayo Clínico
CPD	Centro de Proceso de Datos
HC	Historia Clínica
HCE	Historia Clínica Electrónica
HIP	Hoja de Información al Paciente
HIS	Sistema de Información Clínica
IP	Investigador Principal
LAP	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
LIB	Ley 14/2007, de 3 de julio, de Investigación Biomédica
LIS	Sistema de Información del Laboratorio
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
PACS	Sistema de Archivo y Comunicación de Imágenes Médicas
PHIS	Sistema de Información de la Farmacia Hospitalaria
RDCMDIC	Real Decreto de Conjunto Mínimo de Informes y Documentación Médica
RD-ECM	RD 1090/2015, de 4 de diciembre, por el que se regulan los Ensayos Clínicos con Medicamentos, los Comités de Ética de la Investigación con medicamentos (CEIm) y el Registro Español de Estudios Clínicos
RDLOPD	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

RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
HCDSNS	Historia Clínica Digital del Sistema Nacional de Salud
RIS	Sistema de Información Radiológico - Imágenes médicas
RUE-ECM	REGLAMENTO (UE) 536/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre los Ensayos Clínicos de Medicamentos de uso humano
SNS	Sistema Nacional de Salud
TIC	Tecnologías de la Información y las Comunicaciones

Plan de inspección sectorial de oficio Hospitales Públicos