AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

PLAN DE INSPECCIÓN DE OFICIO SOBRE TRATAMIENTO DE DATOS PERSONALES EN LABORATORIOS HOSPITALARIOS

CONCLUSIONES Y RECOMENDACIONES

Diciembre de 2004

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ÍNDICE

1. INTRODUCCIÓN

El artículo 37 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece entre las funciones de la Agencia de Protección de Datos la de *"velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos"*.

Por su parte, el artículo 28 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, establece que "compete, en particular, a la Inspección de Datos efectuar inspecciones, periódicas o circunstanciales, de oficio o a instancia de los afectados, de cualesquiera ficheros de titularidad pública o privada"*.*

Durante el último trimestre del año 2003 y el primero del 2004, por acuerdo del Director de la Agencia Española de Protección de Datos (APD), se procedió a realizar un Plan de Inspección de oficio al objeto de comprobar el grado de adecuación de los ficheros automatizados utilizados en laboratorios hospitalarios para gestionar los datos personales de los pacientes y en especial su tratamiento por parte de las empresas externas que mantienen sus sistemas de información, a las prescripciones de la Ley Orgánica 15/1999, de 13 de diciembre (LOPD) y normativa que la desarrolla.

Para seleccionar los hospitales y entidades de mantenimiento externas a los mismos que serían objeto de inspección se tomó como punto de partida las inspecciones de oficio a hospitales de titularidad pública que se realizaron en 1996, pues en ellas se detectó la presencia en los laboratorios de entidades externas que permanecían conectadas a los mismos durante las 24 horas del día al objeto de prestar un servicio de atención continuado y facilitar más rápidamente las soluciones a problemas planteados o detectados por los usuarios, todo ello sin control por parte de los responsables de los sistemas de información de los citados laboratorios. Los ficheros con posibilidad de acceso por parte de estas entidades externas contenían datos personales relacionados con la salud de los pacientes.

Las conclusiones que se recogen en el presente documento son el resultado de las inspecciones realizadas en 3 Gerencias de hospital, 14 laboratorios hospitalarios y 6 entidades de mantenimiento de sus sistemas de información, externas a los hospitales de los cuales dependen los citados laboratorios.

Por último debe puntualizarse que el presente informe recoge fundamentalmente aquellos aspectos concretos que son susceptibles de mejoras y que han sido obtenidos de entre todas las inspecciones realizadas, sin que pueda deducirse que los responsables o encargados de tratamiento de los ficheros inspeccionados presenten un funcionamiento deficiente.

2. DESCRIPCIÓN DEL SECTOR

Cada uno de los laboratorios hospitalarios inspeccionados tienen dependencia funcional y orgánica de la Gerencia del hospital al cual pertenecen, que, a su vez, como hospitales públicos que son, dependen de sus respectivas Consejerías de Salud.

Los sistemas de información de los laboratorios tratan datos de carácter personal relativos a la salud de pacientes del propio hospital o su área de influencia y han sido suministrados e implantados por entidades externas a los hospitales, quienes, además, realizan el mantenimiento de los mismos. Normalmente dicho mantenimiento se realiza de forma presencial siempre con asistencia de representantes del laboratorio, aunque, por otra parte, alguna de las entidades inspeccionadas también presta servicios de telemantenimiento.

Los citados sistemas de información ocasionalmente obtienen datos demográficos de los pacientes a partir de los sistemas de información hospitalarios centrales. Sin embargo funcionan de forma independiente y no suelen ser atendidos por los propios servicios de informática centrales.

Las aplicaciones informáticas o aplicativos que manejan dichos sistemas de información normalmente han sido suministrados por las empresas que proveen a los laboratorios hospitalarios de productos propios de laboratorio como son los reactivos u otro tipo de material, como valor añadido en las ofertas relativas a los concursos publicados por los hospitales para la adquisición de dicho material.

Respecto a la disponibilidad de datos de los laboratorios en las entidades de mantenimiento, la Dirección-Gerencia de dos de los tres hospitales de los cuales dependen los 14 laboratorios inspeccionados asumen que es técnicamente posible que dichas entidades dispongan de datos de carácter personal del hospital sin que éste tenga constancia de ello.

Las conclusiones que se recogen en el presente documento se refieren fundamentalmente a aspectos relacionados con la seguridad de los datos tratados por los laboratorios, datos que se refieren a la salud de los afectados y que son considerados especialmente protegidos por la LOPD, por lo que deben gozar de un nivel mayor de seguridad tal y como especifica el Reglamento de Medidas de Seguridad. También se incluyen aspectos relativos a la confidencialidad de los datos tratados como son el deber de secreto y el acceso a los datos por cuenta de terceros. Finalmente se han incluido aspectos formales relativos a la inscripción de ficheros en el Registro General de Protección de Datos y el ejercicio de los derechos de los afectados.

Dichas conclusiones se han obtenido a partir de las actuaciones realizadas en los laboratorios y entidades inspeccionadas. Sin embargo, debe tenerse en cuenta que los proveedores de estos servicios cuentan con cerca de 900 centros y dependencias sanitarias que utilizan uno o mas de los aplicativos inspeccionados, por lo que pueden serles aplicables las presentes conclusiones y recomendaciones.

3. CONCLUSIONES

A continuación, se analiza, desde el punto de vista de la protección de datos, el cumplimiento de cada uno de los principios legales respecto de los tratamientos que realizan los laboratorios y entidades inspeccionadas con los datos personales de los pacientes. Para mayor claridad se diferencian las situaciones de los laboratorios hospitalarios inspeccionados y de las entidades de mantenimiento.

Como se ha señalado, uno de los objetivos básicos del presente Plan consiste en analizar las aplicaciones informáticas que los proveedores facilitan a los laboratorios, así como los servicios de mantenimiento que les prestan. Dado que tales actuaciones suponen el acceso a datos sensibles, el aspecto más relevante de esta inspección ha de hacer referencia a las medidas de seguridad implantadas.

3.1 Seguridad de los datos (artículo 9 de la LOPD y Real Decreto 994/1999, de 11 de Junio. Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal)

Todos los laboratorios hospitalarios inspeccionados tratan datos de salud de personas identificadas utilizando para su gestión los aplicativos revisados en las entidades inspeccionadas, por lo que les es de aplicación el nivel alto de seguridad establecido en el Reglamento de Medidas de Seguridad.

Documento de seguridad

- Laboratorios:

  Los hospitales inspeccionados disponen de un Documento de Seguridad general que presenta diferente casuística. En unos casos dicho Documento hace referencia únicamente a los ficheros generales del hospital, no contemplándose los ficheros departamentales, en otros sí se referencian éstos pero en general los responsables de los laboratorios no son conocedores de ello. El último caso es aquél en el que se dispone de un Documento elaborado de modo general por el organismo del que dependen, pero sin cumplimentar todos aquellos apartados en los que cada hospital debe indicar sus características propias teniendo en cuenta los aspectos de la seguridad que pudieran afectar específicamente a los Laboratorios.

- Entidades de mantenimiento:

  Aunque dos de las seis entidades inspeccionadas disponen de un Documento de Seguridad, éste se refiere a ficheros propios. En ninguna de las entidades se ha encontrado documentación que afecte a los aplicativos instalados a sus clientes ni a los posibles accesos a datos de los mismos. Únicamente una de ellas dispone de un documento de uso interno donde se indican las normas de control de documentación y datos procedentes de los hospitales.

  Por otra parte, con carácter general las entidades manifiestan que los responsables de los ficheros son sus clientes siendo estos, por tanto, responsables de aplicar las medidas de seguridad. Sin embargo, en las inspecciones realizadas se ha encontrado una entidad que disponía en sus propios locales de copias de ficheros de sus clientes y otra de ellas ha

manifestado que ocasionalmente dispone también de copias de ficheros de sus clientes aunque a fecha de las inspecciones realizadas no disponía de ninguna de estas copias.

Funciones y obligaciones del personal.

¤ Laboratorios:

En las inspecciones realizadas se ha detectado que generalmente no están definidas las funciones y obligaciones del personal o, si lo están, han sido elaboradas a nivel hospitalario y no han tenido la suficiente difusión pues el personal de los distintos laboratorios de los hospitales inspeccionados no son conocedores de las mismas.

¤ Entidades de mantenimiento:

Con carácter general no existe documentación específica que trate sobre las funciones y obligaciones del personal con acceso a datos de carácter personal. Incluso los empleados de dos de ellas ni tan siquiera han firmado un compromiso de confidencialidad.

Registro de incidencias.

¤ Laboratorios:

Únicamente los laboratorios de uno de los hospitales disponen de dicho registro aunque sin contener todos los datos especificados en el Reglamento de Seguridad. El resto de los laboratorios inspeccionados o no disponen de dicho Registro o bien su personal no tiene acceso al mismo por encontrarse en el organismo del cual dependen.

¤ Entidades de mantenimiento:

Aunque todas las entidades inspeccionadas disponen de un registro de avisos de sus clientes donde anotan el problema comunicado, únicamente tres de las seis entidades inspeccionadas disponen de un Registro de Incidencias en relación con los aplicativos instalados en sus clientes. Sin embargo dicho registro no es completo conforme al citado Reglamento al no contemplar los efectos derivados de la incidencia ni los datos relacionados con una posible recuperación de datos.

Control de acceso. Identificación y autenticación.

¤ Laboratorios:

En las inspecciones realizadas se ha detectado que existe la posibilidad, previa introducción de una contraseña de acceso, de realizar consultas web de resultados analíticos de al menos dos de los laboratorios inspeccionados pertenecientes a otros tantos hospitales. Los facultativos que pueden realizar este tipo de consultas son usuarios que acceden a través de la red propia (Intranet) del Servicio de Salud al que pertenecen los hospitales de los que dependen los laboratorios, siendo posible consultar tanto las analíticas que han sido solicitadas por dichos facultativos como el resto de las analíticas.

Respecto a la gestión de usuarios, todos los laboratorios hospitalarios disponen de perfiles de acceso a los datos con distintos niveles y restricciones, algunos más extensos que otros. Únicamente uno de ellos no realiza ninguna gestión de usuarios, pues la aplicación que utilizan permite el acceso a los datos sin ningún tipo de identificación ni autenticación. Por otra parte, no todos los laboratorios hospitalarios inspeccionados disponen de una relación escrita de usuarios con acceso a datos personales.

En lo referente a la utilización y gestión de contraseñas, en todos los laboratorios hospitalarios es necesaria la introducción previa de un código de usuario y de una contraseña para acceder a los datos. Aunque en uno de los laboratorios sólo se piden estos datos en el arranque del ordenador, en el resto de los laboratorios hospitalarios inspeccionados se exige tanto para esta operación como para la utilización del aplicativo correspondiente. La caducidad de dichas contraseñas sólo se controla en dos de los laboratorios inspeccionados.

Los intentos fallidos de acceso a los sistemas de gestión de los laboratorios se controlan en todos los laboratorios hospitalarios inspeccionados excepto en dos de ellos. Sin embargo, tras agotar el número límite de intentos establecido en cada uno de ellos, únicamente es necesario reiniciar el aplicativo para disponer de nuevo del mismo número de intentos para poder acceder a los datos.

Respecto al almacenamiento de las contraseñas, todos los aplicativos inspeccionados almacenan las contraseñas de forma cifrada excepto el utilizado en uno de los laboratorios.

Con carácter general los usuarios de laboratorios de los aplicativos inspeccionados disponen de un par usuario-contraseña único por usuario. Sin embargo en tres de los laboratorios inspeccionados disponen de contraseñas genéricas utilizadas por más de un usuario.

- Entidades de mantenimiento:

De las entidades de mantenimiento inspeccionadas sólo dos prestan los servicios de telemantenimiento, una de ellas previo aviso al laboratorio hospitalario para que éste permita el acceso y la otra con acceso libre, es decir, conectándose al laboratorio sin aviso previo. El resto de las entidades realizan el mantenimiento de forma presencial con asistencia de representantes de los laboratorios. En ambas modalidades de mantenimiento el personal técnico de dichas entidades dispone de claves de acceso con perfil de administrador del sistema, lo cual supone libre acceso a todo el sistema de información de los laboratorios.

Una de las entidades inspeccionadas ha incorporado a un fichero los códigos de usuario y contraseñas que le permiten conectarse con sus clientes. El acceso a este fichero se encuentra protegido por una contraseña distinta. Sin embargo, una vez que se accede al mismo las contraseñas son legibles.

Por otra parte únicamente en una de ellas se encontraban ficheros de sus clientes, no disponiendo tampoco de una relación de usuarios autorizados con acceso a los datos contenidos en dichos ficheros.

Gestión de soportes

- Laboratorios:

Con carácter general se ha observado en los laboratorios inspeccionados que no se dispone de una gestión de soportes conforme al Reglamento de Medidas de Seguridad o bien ésta es incompleta. Así, en las inspecciones realizadas se han encontrado a nivel general inventarios de equipos físicos informáticos (servidores, impresoras, etc.), sin que los mismos contengan una

relación de soportes externos a los equipos informáticos donde pudieran guardarse datos de carácter personal obtenidos, como por ejemplo, una copia de respaldo.

Tampoco se dispone en los laboratorios de ningún Registro de Entrada / Salida de soportes, en algunos casos porque, según sus propias manifestaciones, no existe movimiento de aquellos.

Por otra parte, aunque algún Documento de Seguridad a nivel general del hospital pueda contemplar procedimientos relativos a procesos de desecho o reutilización de soportes, éstos no son conocidos en los Laboratorios pues, con carácter general, sus representantes han manifestado que no disponen de ellos.

También se ha constatado que el almacenamiento de soportes no siempre se realiza en un lugar con acceso restringido, como exige el Reglamento.

- Entidades de mantenimiento:

  Sólo en una de estas entidades se ha detectado la existencia de soportes con datos de carácter personal provenientes de sus clientes, disponiendo de una gestión de soportes que incluye el almacenamiento de los mismos en un lugar con acceso restringido, registro de entrada / salida (aunque no contienen la totalidad de los datos especificados en el Reglamento de Seguridad) e identificación del contenido. Así mismo se registran las destrucciones de soportes que se realizan.

  El resto de las entidades inspeccionadas no dispone de una gestión de soportes conforme a las especificaciones del citado Reglamento, aunque algunas de ellas no obtienen soportes de sus clientes.

Copias de respaldo y recuperación

- Laboratorios:

  Los laboratorios hospitalarios inspeccionados realizan copias de seguridad con carácter diario, la mayoría, y semanal, el resto. Además, con carácter general, dichas copias se encuentran almacenadas en lugar distinto al que se encuentran los equipos informáticos.

  Sin embargo se han encontrado tres laboratorios que dejan las copias de respaldo ubicadas en el mismo ordenador donde se realizan. Incluso la copia de uno de ellos se encuentra en una cinta magnética instalada permanentemente en el servidor, que no se ha reemplazado en un año.

- Entidades de mantenimiento:

  Sólo se han encontrado copias de ficheros de sus clientes en una de las entidades inspeccionadas, que son utilizadas con la finalidad de realizar alguna tarea de mantenimiento.

Responsable de seguridad

- Laboratorios:

  Con carácter general las funciones del responsable de seguridad son asumidas por el responsable del propio laboratorio sin existir ninguna mención ni descripción de funciones por escrito al respecto.

Por otra parte sólo en uno de los hospitales a los cuales pertenecen los laboratorios inspeccionados existe la figura del responsable de seguridad a nivel general del hospital cuyas funciones son asumidas por el responsable del servicio de informática, no existiendo dicha figura en el resto de los hospitales.

- Entidades de mantenimiento:

  En estas entidades la situación es algo variada. En algún caso sí existe nombrada la figura del responsable de seguridad, mientras que en otros no está nombrada siendo asumidas sus funciones por el responsable del departamento de Informática. En un caso no existe esta figura.

Auditoría

- Laboratorios:

  Dos de los hospitales de los cuales dependen los laboratorios inspeccionados están a la espera de la finalización de las auditorías encargadas por sus respectivos Servicios de Salud autonómicos que abarcan sus propias redes hospitalarias. Sin embargo uno de estos hospitales dispone de una auditoría de noviembre de 2001 cuyo informe no es completo respecto del Reglamento de Medidas de Seguridad.

  El tercer hospital dispone de una auditoría realizada en mayo de 2002 en la cual se indican las siguientes deficiencias a subsanar: inexistencia de un Documento de Seguridad y documentación relativa a las funciones y obligaciones del personal, inexistencia de un Registro de Incidencias, inexistencia de una estructura de identificación y autenticación que garantice los requisitos exigidos por la Ley (listado actualizado de usuarios con acceso autorizado al sistema de información, gestión de contraseñas, etc.), controles de acceso físico débiles, inexistencia de registros de acceso físico, inexistencia de una gestión de soportes (política de identificación de soportes, cifrado de datos en soportes, control de acceso a soportes, registros de entrada / salida, etc.), realización de pruebas con datos reales. Además la Organización no cuenta con ningún mecanismo que garantice la seguridad de los datos que viajan por redes de comunicaciones públicas. También se indica que «No se descarta asimismo la posible configuración "personal" de usuarios que accedan en remoto desde sus casas y equipos portátiles a servidores departamentales conectados a la red del hospital, ni tampoco el uso de facilidad del correo para otras comunicaciones profesionales que se realicen y que supongan el intercambio de datos personales».

- Entidades de mantenimiento:

  Con carácter general no se han realizado auditorías para verificar el cumplimiento de lo dispuesto en el Reglamento de Seguridad. Sin embargo una de las entidades dispone de auditorías relativas a sus aplicativos en las que se informan de la adaptación a las medidas de seguridad especificadas en el Reglamento antes citado, concretamente de una versión de uno de sus aplicativos, no existiendo dichas medidas en versiones anteriores.

Control de acceso físico

- Laboratorios:

  Ninguno de los laboratorios inspeccionados dispone de controles de acceso físico ni de relación de personas con autorización de acceso. Se da además la circunstancia de que los servidores se encuentran ubicados en zonas de los laboratorios de libre acceso. Por otra parte, aunque generalmente los laboratorios permanecen cerrados con llave tras la

  finalización de la jornada laboral, los laboratorios de uno de los hospitales, cuya jornada finaliza a las tres de la tarde, permanecen abiertos a la espera de la realización de las tareas de limpieza cerrándose el paso una vez finalizadas éstas, sobre las nueve de la noche.

Pruebas con datos reales

- Entidades de mantenimiento:

  Las entidades inspeccionadas responsables de las aplicaciones utilizadas en los laboratorios no realizan pruebas con datos reales. Únicamente una de ellas utiliza datos reales anonimizados para probar el funcionamiento respecto a las diferentes casuísticas de los laboratorios, asignando para ello una identificación personal ficticia.

Distribución de soportes

- Laboratorios y Entidades de mantenimiento:

  Con carácter general, los distintos aplicativos inspeccionados implantados en los laboratorios hospitalarios, no disponen de una opción que permita cifrar los datos que se obtienen en un soporte externo. Únicamente un aplicativo de una de las entidades dispone de una opción al respecto aunque sólo en una de sus versiones que se encuentra disponible en 42 de sus 496 clientes. Sin embargo, a fecha de la inspección realizada, dicha entidad tenía en su poder ficheros en soporte magnético de ocho clientes, seis de los cuales contenían datos de salud de pacientes identificados, todos ellos sin cifrar.

Registro de accesos

- Laboratorios:

  Los distintos aplicativos implantados en los laboratorios hospitalarios inspeccionados pueden disponer o no de registro de accesos. Sin embargo, con carácter general, los representantes de dichos laboratorios desconocen su existencia por lo que difícilmente se pueden detectar accesos indebidos así como realizar revisiones periódicas y elaborar informes de problemas detectados, conforme a lo especificado en el artículo 24 del Reglamento de Medidas de Seguridad.

- Entidades de mantenimiento:

  Se observa en dichas entidades una tendencia a incluir el registro de accesos requerido por el Reglamento de Seguridad en sus aplicativos. Así, cuatro de ellas ya lo implementan en las nuevas versiones de sus aplicativos. Las otras dos entidades inspeccionadas, también disponen de este registro en sus aplicativos. Sin embargo únicamente se guardan en él los movimientos de registros relativos a altas, bajas y modificaciones, no grabándose las consultas realizadas.

  Sin embargo, aunque con carácter general los nuevos aplicativos ya disponen de registro de accesos conforme a las especificaciones del mencionado Reglamento, todavía quedan numerosos centros sanitarios que no tienen instaladas las versiones que lo implementan pues la actualización de versión es decisión de dichos centros y no de las entidades citadas.

  Así, teniendo en cuenta el número total de clientes de las entidades, se puede suponer que al menos 500 de ellos, no disponen de registro de accesos y, al menos 19, aunque disponen de dicho registro, en él no se almacenan las consultas realizadas.

Telecomunicaciones

- Laboratorios:

Con carácter general los responsables de los laboratorios hospitalarios inspeccionados desconocen si las transmisiones de datos se realizan cifrando los datos. Por otra parte, en las inspecciones realizadas se ha comprobado que es posible consultar informes analíticos de pacientes identificados de algunos de los laboratorios a través de una red Intranet o a través de Internet. La conexión se realiza con protocolo no seguro “http” sin existir cifrado datos.

- Entidades de mantenimiento:

  Únicamente dos de los aplicativos de los ocho inspeccionados, disponen de utilidades que permitan cifrar los datos ante una transmisión electrónica de los mismos.

  Por otra parte, en la conexión de una de las entidades que prestan servicios de telemantenimiento y que da servicio al menos a cuatro de los laboratorios inspeccionados, los datos no se transmiten cifrados. Así mismo, el aplicativo de una de las entidades dispone de un módulo de utilización intrahospitalaria que habilita el acceso a resultados asociados a las analíticas a través de un navegador web y permite la comunicación utilizando un canal no seguro.

3.2 Deber de Secreto (artículo 10 de la LOPD)

- Laboratorios:

  Con carácter general, en los hospitales inspeccionados de los cuales dependen los laboratorios inspeccionados, bien desde la Dirección del centro o desde el Servicio de Informática, se ha promovido la difusión del deber de secreto a que están obligadas las personas que tratan datos de carácter personal, mediante la elaboración y distribución de documentos informativos a los distintos servicios hospitalarios o la información ofrecida al respecto en las distintas jornadas organizadas. Incluso uno de los hospitales ha elaborado un modelo de compromiso de confidencialidad que ha incluido en el Documento de Seguridad.

  Sin embargo parece que esta información no ha llegado a los usuarios finales de los datos pues de los 14 laboratorios inspeccionados, únicamente en uno de ellos su responsable ha solicitado a los mismos la firma de un compromiso de confidencialidad, mientras que en el resto de los laboratorios la existencia de dicho documento es desconocida por los usuarios, quienes no han suscrito el citado compromiso.

- Entidades de mantenimiento:

  En cuanto a las seis entidades suministradoras de aplicativos inspeccionadas, los empleados con acceso a datos personales de dos de ellas no han firmado un compromiso de confidencialidad específico o incluido alguna cláusula al respecto en el contrato laboral, en uno de los casos por considerar la entidad que dicho compromiso se encuentra incluido dentro del ámbito de la buena fe contractual.

3.3 Acceso a los datos por cuenta de terceros (Artículo 12 de la LOPD)

- Laboratorios:

  La contratación de los aplicativos instalados en los 14 laboratorios hospitalarios inspeccionados está en función de las gestiones realizadas por los equipos de dirección de los hospitales de los cuales dependen. Normalmente dichos aplicativos son incluidos como un elemento de valor

añadido en las ofertas de los proveedores que concurren a las convocatorias de los hospitales para la adquisición de reactivos necesarios en la realización de técnicas analíticas. Sin embargo, en algunas ocasiones el hospital suscribe un documento en el que figura la cesión o uso en precario de las citadas aplicaciones al margen de los contratos celebrados, o su instalación y mantenimiento.

En la documentación contractual existente entre los hospitales y las entidades contratadas (pliegos de concursos, en su caso contratos, etc.) en general no se han encontrado expresamente las especificaciones del artículo 12 de la LOPD, aunque sí existen algunos compromisos de confidencialidad al respecto. Únicamente uno de los hospitales dispone de contratos que contienen expresamente dichas garantías, pues algunos de ellos fueron actualizados con posterioridad a su firma, quedando otros pendientes de actualizar.

Por otra parte, dos de los hospitales han desarrollado un modelo de contrato para regular el acceso por terceros a los ficheros de los Laboratorios que contengan datos de carácter personal, incluyendo las garantías exigidas por el artículo 12 de la LOPD.

- Entidades de mantenimiento:

Con carácter general prestan los servicios de mantenimiento de sus aplicativos instalados en laboratorios de forma presencial, a excepción de dos de ellas que realizan servicios de telemantenimiento. En algunas disponen en sus instalaciones de copias de los ficheros hospitalarios para realizar tareas concretas de mantenimiento, en cuyo caso se firma un "documento de cesión de datos" donde se identifica al receptor de los datos en dicha empresa y quién hace la entrega por parte del cliente.

A pesar de haber obtenido la información indicada para los hospitales con respecto a las entidades inspeccionadas, en las inspecciones realizadas en éstas se ha solicitado documentación contractual entre ellas y otros 43 centros sanitarios con los que, también, mantienen una relación similar, al objeto de verificar que se cumplen las garantías del artículo 12 de la LOPD, comprobándose que, a excepción de uno de los contratos, el resto carecía de las mismas. Por otra parte, los representantes de una de las entidades han manifestado que nunca suscriben contratos para la utilización de su aplicativo pues éste se instala al margen de los contratos celebrados.

3.4 Derechos de las personas: acceso, rectificación, cancelación y oposición (Artículos 15 y 16 de la LOPD).

- Laboratorios:

Ninguno de los hospitales de los cuales dependen los laboratorios inspeccionados dispone de procedimientos escritos para atender los derechos de los afectados reconocidos en la LOPD y en 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.

- Entidades de mantenimiento:

Con carácter general tampoco disponen de este tipo de procedimientos por entender que es el responsable del fichero quien se encuentra obligado por dicha norma legal.

3.5 Creación, modificación o supresión de ficheros. Notificación e inscripción registral. (Artículos 20, 25 y 26 de la LOPD)

¤ Laboratorios:

Dos de los hospitales se encuentran en fase de revisión de la inscripción de sus ficheros, estando pendiente, en el caso de uno de ellos, la publicación en el Boletín de la Comunidad Autónoma de la correspondiente orden de creación de los mismos. El tercer hospital tiene inscritos los ficheros denominados “Historias clínicas” y “Usuarios del sistema sanitario”.

¤ Entidades de mantenimiento:

Sólo una de ellas disponía en sus locales de ficheros de sus clientes, con el fin de realizar alguna tarea de mantenimiento. Sin embargo, según manifestaciones de sus representantes, dicha empresa no ha inscrito ninguno de estos ficheros por entender que es responsabilidad de sus propios clientes.

4. RECOMENDACIONES

A la vista de las anteriores conclusiones deben formularse las siguientes recomendaciones:

PRIMERA: SEGURIDAD DE LOS DATOS

El artículo 9 de la LOPD establece:

“*1. El responsable del fichero y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.”.

En las inspecciones realizadas se ha comprobado la existencia de deficiencias en materia de seguridad por lo que se recomienda la revisión de los documentos de seguridad existentes, así como de las medidas de seguridad implantadas, al objeto de que se adecuen a los distintos artículos del Reglamento de Medidas de Seguridad debiendo, específicamente, considerar los siguientes aspectos:

Documento de seguridad.

¤ Laboratorios:

El artículo 8 del Reglamento de Medidas de Seguridad obliga al responsable del fichero a elaborar e implantar la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

Este Documento debe contener una serie de aspectos incluidos en los artículos 8 y 15 del Reglamento ya que, al tratarse datos de salud, son exigibles, además de las medidas de seguridad de nivel alto, las de nivel básico y medio.

El Documento de Seguridad debe hacer referencia a todos los ficheros con datos de carácter personal del centro. Así mismo, debe ser completo y contemplar las exigencias de los citados artículos pues en las inspecciones realizadas se ha comprobado que, además de las deficiencias encontradas, alguno de los Documentos de Seguridad revisados no contenían las estructuras de registro ni la descripción de los sistemas de información asociados, como se especifica en el artículo 8.2.d) del citado Reglamento.

Por tanto, los hospitales deben disponer de un Documento de Seguridad completo y adaptado a la situación real de los mismos.

¤ Entidades de mantenimiento:

Ninguna de las entidades inspeccionadas dispone de un documento relacionado con la seguridad para el tratamiento de los datos de carácter personal de los hospitales que son sus clientes por no encontrarse normalmente en posesión de sus datos personales.

Sin embargo, dado que en las inspecciones realizadas se ha detectado la presencia en alguna entidad de ficheros de sus clientes, éstas deben disponer de un Documento de Seguridad, especificando aquellas medidas que les sean de aplicación como consecuencia de los accesos a los datos hospitalarios que realizan, medidas que han de tener mayor amplitud en las entidades con posibilidad de acceso remoto a los datos hospitalarios para realizar las tareas de telemantenimiento, en las cuales además, debería estar controlado el acceso físico a los locales donde se encuentren los equipos desde los que sea posible el acceso a los datos de los hospitales.

Además, debe reiterarse que, conforme a lo especificado en el artículo 9.2 del Reglamento de Medidas de Seguridad, las normas de seguridad que afectan al desarrollo de las funciones del personal con acceso a datos de carácter personal deben ser conocidas por el mismo.

Funciones y obligaciones del personal.

¤ Laboratorios:

Conforme a lo especificado en el artículo 9 del Reglamento de Medidas de Seguridad, las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información deben estar claramente definidas y documentadas, debiendo adoptar el responsable, las medidas necesarias para que todo el personal conozca cuáles son sus funciones y obligaciones así como las normas de seguridad que afecten al desarrollo de las mismas y las consecuencias derivadas de su incumplimiento.

La definición de las funciones y obligaciones del personal realizadas por los hospitales deben incluir también a las entidades de mantenimiento de los aplicativos en su condición de usuarios con acceso a datos personales.

¤ Entidades de mantenimiento:

Las funciones y obligaciones del personal de dichas entidades con acceso a datos de los laboratorios hospitalarios deben estar igualmente definidas y documentadas así como difundidas entre el personal afectado por las mismas.

Registro de incidencias.

- Laboratorios:

  Conforme a lo especificado en los artículos 10 y 21 del Reglamento de Medidas de Seguridad los laboratorios hospitalarios deben disponer de un Registro de Incidencias que contenga al menos: tipo de incidencia, fecha y hora en la que se ha producido, persona que realiza la notificación, persona a quién se notifica y efectos derivados. Así mismo, cuando sea necesario realizar una recuperación de datos se deben guardar, además, los procedimientos de recuperación de datos aplicados, la identificación de la persona que realizó el proceso de recuperación de datos, los datos que se han restaurado, en su caso, los datos que ha sido necesario grabar manualmente y la persona que autoriza la ejecución de los procedimientos de recuperación de datos de la que debe constar su firma. Así mismo debe existir una autorización escrita del responsable del fichero para ejecutar los procedimientos de recuperación de los datos.

  Las incidencias pueden afectar tanto a la ubicación lógica como física de los datos personales, por lo que el responsable directo de los datos debe ser conocedor de las mismas a fin de proponer, elaborar e implantar las medidas y procedimientos de subsanación de las mismas en los casos que proceda, lo que difícilmente puede realizarse sin realizar un análisis periódico del Registro de Incidencias.

- Entidades de mantenimiento:

  Las entidades que en algún momento traten en sus locales copias de los ficheros de sus clientes, deberán disponer de un Registro de Incidencias conforme a lo especificado en los artículos 10 y 21 del Reglamento citado.

Control de acceso - Identificación y autenticación.

Los artículos 11 y 12 del Reglamento de Medidas de Seguridad establecen la obligatoriedad por parte de los responsables de ficheros con datos personales de disponer de una serie de mecanismos que impidan que usuarios no autorizados accedan a este tipo de datos. Además deben disponer de una relación de usuarios con acceso autorizado a los datos de carácter personal en la que se especifique el tipo de acceso autorizado para cada uno de ellos, así como establecer procedimientos de identificación y autenticación para dicho acceso.

El artículo 11 de dicho Reglamento también especifica que cuando el mecanismo de autenticación se base en la existencia de contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento de las mismas que garantice su confidencialidad e integridad. Dichas contraseñas deberán ser cambiadas periódicamente y almacenadas de forma ininteligible.

Por otra parte, el artículo 18 del citado Reglamento especifica que los usuarios que accedan a datos de carácter personal deberán poderse identificar de forma inequívoca y personalizada, verificándose que están autorizados para dicho acceso. Así mismo, debe limitarse la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

- Laboratorios:

  Los laboratorios deben elaborar una relación de usuarios actualizada en la que se especifique el acceso autorizado para cada uno de ellos. El tipo de acceso puede ser personalizado

para cada usuario o bien pueden definirse previamente una serie de perfiles de acceso dependiendo de las necesidades específicas de cada puesto de trabajo y posteriormente asignar un perfil a cada usuario.

Respecto a la gestión de contraseñas, dada la confidencialidad de las mismas, la buena práctica aconseja que nadie, ni siquiera el administrador del sistema tenga acceso a ellas, así como que al producirse el primer acceso se obligue al usuario a cambiar la contraseña que inicialmente entregó el administrador y que dichas contraseñas, no sólo se almacenen de forma cifrada sino también que se visualicen de la misma forma y que no aparezcan en las relaciones de usuarios con acceso a datos personales. Además, para cumplir con lo especificado en el artículo 11.3 del Reglamento de Seguridad es aconsejable establecer procedimientos que garanticen que las contraseñas se cambien periódicamente. Así mismo se considera buena práctica que el sistema de acceso a los datos se desconecte automáticamente tras un tiempo de inactividad previamente definido.

Cuando existan usuarios genéricos en algunos de los laboratorios hospitalarios inspeccionados, se deberá proceder a la eliminación de dichos usuarios creándose unos nuevos que permitan la identificación inequívoca y personalizada de cada uno de ellos.

Por otra parte, limitar a una cantidad determinada los intentos de acceso indebido a los datos puede no ser suficiente si, tras agotar esa cantidad, lo único que hay que hacer es reiniciar de nuevo el sistema. Por ello, se considera buena práctica que, una vez agotado el número máximo de intentos fallidos establecido, el usuario quede bloqueado y sea el administrador el que asigne una nueva contraseña comenzando de nuevo el proceso de obligación de cambio de contraseñas en la primera conexión.

Respecto a las tareas de telemantenimiento, los laboratorios deben ser quienes en todo momento controlen los accesos de las entidades que prestan tal servicio. Por ello, no debe existir la posibilidad de que dichas entidades puedan conectarse sin conocimiento de los primeros. A tal efecto la posibilidad de conexión no debe encontrarse disponible permanentemente sino sólo en el momento en que sea necesaria la intervención de la citada entidad y siempre con conocimiento del laboratorio. Además, el acceso realizado por la entidad de mantenimiento, al igual que otros accesos, debe quedar reflejado en el Registro de Accesos tal y como se especifica en el artículo 24 del Reglamento de Seguridad. Así mismo, para asegurar que un usuario se conecta desde el lugar previamente definido, una conducta de buena práctica sería establecer un procedimiento de retrollamada automática (*call back*) de tal forma que cuando la entidad conecte con el laboratorio éste realice una llamada al número de la entidad establecido para la conexión, evitando así las conexiones no autorizadas desde puntos externos de acceso.

- Entidades de mantenimiento:

Cuando las entidades de mantenimiento de los aplicativos instalados en los laboratorios dispongan de copias de ficheros de sus clientes, deberán disponer, en relación a dichos ficheros, de la correspondiente relación de usuarios con acceso a ellos, así como observar lo dispuesto en los artículos 11, 12 y 18 del Reglamento.

Por otra parte, en relación a los accesos realizados por dichas entidades cuando prestan los servicios de telemantenimiento, las contraseñas de acceso a datos de sus clientes de que dispongan deben almacenarse de forma ininteligible conforme a lo especificado en el artículo 11.3 del Reglamento de Seguridad.

Gestión de soportes.

- Laboratorios:

  Conforme a las especificaciones de los artículos 13 y 20 del Reglamento de Seguridad los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado, el cual estará relacionado en el documento de seguridad. Este tipo de soporte únicamente podrá salir fuera de los locales en los que esté ubicado el fichero con una autorización del responsable del mismo.

  Se establece también la obligación de crear un registro de entrada / salida de soportes que contenga: tipo de soporte, fecha y hora, emisor / destinatario, número de soportes, tipo de información que contienen, forma de envío y la persona responsable de la recepción / entrega que deberá estar debidamente autorizada.

  El artículo 20 del Reglamento en sus apartados 3 y 4 obliga a adoptar medidas para impedir cualquier recuperación posterior de la información almacenada en él cuando un soporte vaya a ser desechado o reutilizado, previamente a que se proceda a su baja en el inventario, y a adoptar las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos cuando vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de las operaciones de mantenimiento.

  A tal efecto, el calificativo “informático” aplicado a los soportes no aparece referido específicamente en los citados apartados del artículo 20, sin embargo el artículo 2.10 del Reglamento considera “soporte” al objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos. El precepto no distingue entre soportes informáticos o no, sino que resulta omnicomprensivo de todos ellos en congruencia con los preceptos de la LOPD, que tratan de evitar accesos no autorizados a los datos cualquiera que sea el procedimiento u operación para llevarlo a cabo.

  A este respecto los hospitales deberán, además de elaborar normas generales sobre procedimientos de gestión de soportes, vigilar la efectiva implantación de dichas medidas. Estas normas deberán contemplar todas las especificaciones de los citados artículos 13 y 20 del Reglamento de Medidas de Seguridad.

  A nivel departamental, los laboratorios hospitalarios así como todas las unidades del hospital donde se traten datos personales de nivel medio o alto deberán elaborar inventarios completos de soportes con datos personales (discos duros, soportes magnéticos externos de todo tipo, etc.) identificando su contenido y guardándolos en un lugar con acceso restringido.

  Así mismo, en todo momento deberán gestionar un Registro de Entrada / Salida con los datos especificados anteriormente y anotar en él todos los movimientos físicos que se realicen con dichos soportes, incluso si salen de los locales de ubicación del fichero con la única finalidad de la realización de tareas de mantenimiento. Cualquier salida de soportes con datos de carácter personal fuera de los locales de ubicación del fichero, debe ser autorizada por el responsable del mismo. Es preciso insistir, a la vista de la experiencia, en la necesidad de adoptar medidas para impedir una recuperación de los datos contenidos en los soportes cuando vayan a ser desechados o reutilizados, teniendo en cuenta dar la correspondiente baja en el inventario en el primer caso.

  Por otra parte, al desechar la información en soportes en papel deberá procederse a su destrucción impidiendo que sea reutilizada.

- Entidades de mantenimiento:

Aquellas entidades que en algún momento disponen en sus locales de copias de los ficheros de sus clientes, deberán realizar una gestión de soportes conforme a las especificaciones de los artículos 13 y 20 del Reglamento de Seguridad.

Copias de respaldo y recuperación.

¤ Laboratorios:

Dentro de las medidas de nivel básico, el Reglamento de Seguridad especifica que los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción, siendo el responsable del fichero quien se encargue de verificar la definición y correcta aplicación de dichos procedimientos. Además, las copias de respaldo deberán realizarse al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Estas medidas se ven reforzadas en los casos en que son exigibles las medidas de nivel alto en cuyo caso deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan, sin que puedan guardarse en el mismo ordenador donde se hayan obtenido.

Una conducta de buena práctica aconseja realizar las copias de respaldo en distintos soportes de forma que se utilicen alternativamente y así poder asegurar una recuperación de datos cuando se detecte una pérdida de los mismos tras un período superior al establecido para la realización de dichas copias. Además, una copia de respaldo deberá conservarse en lugar diferente de aquél en que se encuentren los equipos informáticos tal y como exige el Reglamento de Seguridad al tratarse de datos de salud.

¤ Entidades de mantenimiento:

No hay recomendaciones al respecto al no ser dichas entidades responsables del fichero.

Responsable de seguridad.

¤ Laboratorios:

El artículo 16 del Reglamento de Medidas de Seguridad establece la obligatoriedad por parte del responsable del fichero de designar uno o varios responsables de seguridad para coordinar y controlar las medidas definidas en el documento de seguridad, sin que esta designación suponga una delegación de la responsabilidad que corresponda al responsable del fichero.

Se considera una buena práctica la no coincidencia entre el responsable de seguridad y el responsable de informática, ya que al primero, según el Reglamento de Seguridad, le corresponderían tareas como coordinar y controlar la implantación de las medidas de seguridad definidas en el Documento de Seguridad, analizar los informes de auditoría y elevar las conclusiones al responsable del fichero proponiendo medidas correctoras y revisar periódicamente el Registro de Accesos, así como, lógicamente, definir la política de seguridad de la entidad, elaborar, revisar y actualizar de Documento de Seguridad, coordinar la implantación de las medidas de seguridad, etc. Por tanto, si coincide el responsable de seguridad con el responsable del departamento de Informática se puede ofrecer una visión no objetiva de la situación al ser dicho departamento parte implicada en el tratamiento de datos

personales y poder plantearse un conflicto de intereses entre sus funciones como responsable del departamento de informática y responsable de seguridad.

- Entidades de mantenimiento:

  Dado que estas entidades pueden acceder a datos de los laboratorios para realizar las tareas de mantenimiento, se recomienda que nombren un responsable de seguridad en relación con dichos accesos que coordine y proponga procedimientos de seguridad y confidencialidad al respecto. Es aconsejable, conforme a la buena práctica, que la figura del responsable de seguridad no coincida con el responsable informático, por las mismas razones expresadas en el párrafo anterior.

Auditoría.

¤ Laboratorios:

El artículo 17 del Reglamento de Medidas de Seguridad obliga a la realización de una auditoría de seguridad interna o externa que verifique el cumplimiento de dicho Reglamento así como de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años. El informe de auditoría debe ser analizado por el responsable de seguridad competente dictaminando sobre la adecuación de las medidas y controles al Reglamento, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias para su adopción por el responsable del fichero.

La auditoría de seguridad se exige a partir de las medidas de nivel medio, que entraron en vigor en fecha 26/6/2000, por lo que los laboratorios que no las hayan realizado deberán efectuarlas con carácter inmediato.

¤ Entidades de mantenimiento:

Las entidades que en algún momento custodien datos de sus clientes o bien realicen tareas de telemantenimiento, deberán realizar una auditoría de seguridad respecto de aquellas medidas que les sean exigibles.

Control de acceso físico.

¤ Laboratorios:

El Reglamento de Medidas de Seguridad establece que exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

A este respecto los hospitales, como responsables de ficheros con datos de carácter personal, deben elaborar una lista de personal con autorización de acceso físico a dichos locales que incluya personal tanto del propio laboratorio como del resto del hospital, así como implantar medidas que impidan que personas no autorizadas puedan acceder a los citados locales.

¤ Entidades de mantenimiento:

Las mismas medidas deberán adoptar dichas entidades cuando dispongan de copias de ficheros de sus laboratorios clientes.

Distribución de soportes.

- Laboratorios y Entidades de mantenimiento:

  Conforme al artículo 23 del Reglamento de Medidas de Seguridad, la distribución de soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

  A tal efecto, los responsables y encargados de tratamiento de ficheros que contengan datos de carácter personal de nivel alto, deben disponer de programas de utilidad internos o externos a los aplicativos que gestionan sus datos, que permitan obtener soportes externos para su distribución de forma que la información en ellos contenida se encuentre cifrada, no siendo inteligible ni manipulada durante su transporte.

Registro de accesos.

- Laboratorios:

  El artículo 24 del Reglamento de Seguridad especifica para los ficheros con nivel de seguridad alto que se debe guardar al menos durante dos años como mínimo la identificación de usuario, fecha, hora, fichero accedido, tipo de acceso y, si ha sido autorizado, también la identificación del registro accedido. Todo ello de cada acceso realizado.

  Por otra parte, tras haberse constatado que algunos de los aplicativos inspeccionados no guardan aquellos accesos en los que sólo se realiza una consulta, se reitera que los hospitales, al serles exigidas las medidas de nivel alto, deberán en todo momento guardar los datos indicados de todos los accesos a datos personales que se realicen, incluidas las consultas.

  Dado que en ficheros con un nivel elevado de consultas esta medida puede afectar negativamente en relación con el volumen de almacenamiento, es conveniente recordar que el Reglamento de Seguridad no obliga a que estos datos se encuentren permanentemente en línea, pudiendo encontrarse almacenados en soportes externos.

  Además, el mismo artículo del Reglamento obliga a revisar periódicamente la información registrada elaborando, al menos una vez al mes, un informe de las revisiones realizadas y los problemas detectados, por lo que los responsables de seguridad de los ficheros de los laboratorios deben poder disponer del citado registro de accesos.

Telecomunicaciones.

- Laboratorios:

  El artículo 26 del Reglamento de Medidas de Seguridad obliga a que las transmisiones de datos de carácter personal a través de redes de telecomunicaciones se realicen cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros; todo ello cuando el nivel de seguridad aplicable sea el *alto.*

  A este respecto, bien desde las propias aplicaciones contratadas en los laboratorios hospitalarios o bien por otros programas ajenos a dichas aplicaciones, debe existir una opción de cifrado de los datos disponible para los usuarios de los mismos al objeto de su utilización en caso de transmisión electrónica.

Las medidas a las que se refiere el artículo 26 del Reglamento, serán de aplicación a la transmisión de datos entre distintas dependencias de la entidad cuando sea necesaria para dicha transmisión la utilización de redes de telecomunicaciones cuya titularidad sea ajena a la propia empresa, no siendo preciso el cifrado de los datos en caso de que las comunicaciones en ningún momento accedan a dicha red.

Por su parte, las consultas web deben realizarse utilizando un protocolo seguro (del tipo *https*).

En cuanto a los accesos realizados como consecuencia de las tareas de telemantenimiento prestado por algunas de las entidades, los responsables de los ficheros deben asegurarse que, en todo momento, los datos viajen cifrados a través de las redes de telecomunicaciones.

SEGUNDA: DEBER DE SECRETO

¤ Laboratorios:

El artículo 10 de la LOPD obliga a todas las personas que intervengan en el tratamiento de datos de carácter personal a guardar secreto profesional respecto de los mismos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Con el fin de que todo el personal que tenga acceso a los datos personales conozca esta obligación, resulta conveniente no sólo la elaboración de documentos informativos y la realización de jornadas y seminarios con tal finalidad, sino también la adopción de medidas dirigidas a su conocimiento por todo el personal como, por ejemplo, la aceptación explícita de un compromiso de confidencialidad.

¤ Entidades de mantenimiento:

Dado que parte del personal de estas entidades accede a datos personales de los laboratorios, el criterio expuesto para ellos será igualmente aplicable a las entidades en relación a los accesos que realizan.

TERCERA: ACCESO A LOS DATOS POR CUENTA DE TERCEROS

El artículo 12.1 de la Ley Orgánica 15/1999 establece que *"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicha acceso sea necesario para la prestación de un servicio al responsable del tratamiento.* Añadiendo los apartados 2 y 3 que indican *"2. 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, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que 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, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento"

El artículo 12.1 de la Ley Orgánica 15/1999 permite que el responsable del fichero habilite el acceso material a datos de carácter personal por parte de la entidad que va a prestarle un servicio -encargado del tratamiento- sin que, por mandato expreso de la ley, pueda considerarse dicho acceso como una cesión de datos.

En tal sentido debe resaltarse que esta habilitación legal supone una importante excepción al principio del consentimiento del afectado que, en el caso de los datos de salud, al ser objeto de protección especial, ha de ser expreso. De ahí la trascendental importancia que *tiene el hecho de que un tercero, sin consentimiento ni conocimiento del afectado, pueda acceder a sus datos de salud.*

Por ello este acceso que la Ley permite debe estar rodeado de un abanico de exigencias que garanticen un correcto tratamiento de la información. De no concurrir estas garantías resulta inaplicable la excepción legal dando lugar a una comunicación ilícita de los datos por el que encarga el servicio y a otra de tratamiento ilegal por el que lo presta. Ambas conductas están tipificadas en la Ley Orgánica como infracciones muy graves.

Esta cuestión ha sido, también, objeto de análisis por la Sala de lo Contencioso Administrativo de la Audiencia Nacional que, en Sentencia de 19 de noviembre de 2003 ha señalado que "para tener la condición legal de encargado del tratamiento, al que por cierto le es de aplicación el régimen sancionador que establece la Ley Orgánica 15/1999, según dispone el artículo 43.1 de la expresada Ley, es necesario cumplir una serie de exigencias necesarias, que operan a modo de garantías, establecidas en el artículo 12 de la Ley Orgánica 15/1999. Así es, cuando el tratamiento se realice por cuenta de un tercero debe constar "por escrito o en alguna otra forma que permita acreditar su celebración y contenido", por lo que no basta con acreditar que existe una relación jurídica entre el responsable del fichero y el encargado del tratamiento, sino que ésta ha de constar por escrito o por otra forma que permita acreditar su "celebración y contenido". En este sentido, la propia Ley prevé un contenido mínimo del contrato entre las partes en el que deben constar una serie de estipulaciones necesarias, a saber, seguir las instrucciones del responsable del tratamiento, no utilizar los datos para un fin distinto, no comunicarlos a otras personas (artículo 12.2 párrafo primero), estipular las medidas de seguridad del artículo 9 (artículo 12.2 párrafo segundo) y cumplida la prestación destruir los datos o proceder a su devolución al responsable del tratamiento (artículo 12.3).

Las garantías a que se hace referencia son las expresamente exigidas por el artículo 12 de la LOPD. En este sentido, la propia Ley prevé un contenido mínimo del contrato entre las partes en el

que deben constar una serie de estipulaciones necesarias, a saber, seguir las instrucciones del responsable del tratamiento, no utilizar los datos para un fin distinto, no comunicarlos a otras personas (artículo 12.2 párrafo primero), estipular las medidas de seguridad del artículo 9 (artículo 12.2 párrafo segundo), y cumplida la prestación destruir los datos o proceder a su devolución al responsable del tratamiento (artículo 12.3).

Respecto de ellas ha de advertirse que, como ha exigido la Agencia Española de Protección de Datos y ha ratificado la Audiencia Nacional, cuando el tratamiento se realice por cuenta de un tercero debe constar "por escrito o en alguna otra forma que permita acreditar su celebración y contenido", por lo que no basta con acreditar que existe una relación jurídica entre el responsable del fichero y el encargado del tratamiento, sino que ésta ha de constar por escrito o por otra forma que permita acreditar su "celebración y contenido".

- Laboratorios:

  A la vista de las inspecciones realizadas se ha podido constatar que con carácter general, o bien no existe contrato entre los hospitales y las entidades a cuyos laboratorios dan soporte, o bien, si existe, normalmente no contienen las especificaciones del artículo 12 de la LOPD.

  Por tanto, a los efectos de cumplir las garantías exigidas por la normativa de protección de datos, tanto los hospitales como las entidades que les dan soporte, deberán, con carácter inmediato y urgente, suscribir, en unos casos, y adecuar, en otros, los contratos de prestación de servicios establecidos con el fin de recoger lo previsto en el artículo 12 de la LOPD. En otro caso deberán cesar en el acceso a la información.

  Por otra parte, en los Pliegos de cláusulas administrativas y Pliegos de prescripciones técnicas relativos a concursos publicados por los hospitales que pudieran implicar el acceso a datos personales por terceros, se deben incluir unos apartados o cláusulas en las cuales se reflejen las anteriores prescripciones legales, de manera que tales Pliegos se ajusten no sólo a lo dispuesto en la Ley de Contratos de las Administraciones Públicas y normas complementarias, sino también a lo establecido en la LOPD y normativa de desarrollo.

  Además, en caso de preverse o producirse una subcontratación que implique tratamiento de datos personales, deberán reflejarse en los citados Pliegos los requisitos exigidos por la LOPD, haciendo constar expresamente que, o bien el contratista adjudicatario del servicio actúa en nombre y por cuenta del responsable del fichero o tratamiento (hospital) o, alternativamente, se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato:

  1. Que los servicios a subcontratar se hayan previsto expresamente en el contrato originario celebrado entre el hospital y el adjudicatario del servicio.
  2. Que el contenido preciso del servicio subcontratado conste en el contrato originario.
  3. Que el responsable del tratamiento establezca las instrucciones mediante las cuales el subcontratista tratará los datos, sin perjuicio de las instrucciones adicionales que pudieran establecerse por el adjudicatario del servicio.
  4. Que en el contrato originario se establezcan las medidas de seguridad a adoptar por el subcontratista, sin perjuicio de las medidas adicionales que pudieran establecerse por el adjudicatario del servicio.

- Entidades de mantenimiento:

Respecto a estas entidades, para que el acceso a los datos de los laboratorios que realizan no constituya infracción contra la LOPD, igualmente deben regular la relación contractual mediante un contrato escrito conforme a las especificaciones del citado artículo 12 de dicha norma.

CUARTA: DERECHOS DE LAS PERSONAS: ACCESO, RECTIFICACIÓN, CANCELACIÓN y OPOSICIÓN

¤ Laboratorios:

La LOPD reconoce los derechos de acceso, rectificación, cancelación y oposición. Respecto al derecho de acceso indica que el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos, obteniendo la información por medio de su visualización, escrito, copia, etc., sin utilizar claves o códigos, no pudiendo ejercer su derecho de acceso a intervalos no inferiores a doce meses, salvo interés legítimo del interesado.

En cuanto a los derechos de rectificación y cancelación, el artículo 16 de la LOPD establece que serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en dicha Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

Sin embargo la regulación de estos derechos se complementa con lo previsto en 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. Conforme a dicha norma debe tenerse en cuenta que el derecho de acceso del paciente a la historia clínica puede ejercerse también por representación debidamente acreditada y que no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

Según dicha Ley los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

En cuanto a la conservación de la documentación clínica (cualquiera que sea el soporte) hay que señalar que deberá ser conservada por un período mínimo de 5 años, conforme a la Ley citada, o durante los períodos mínimos establecidos en la normativa autonómica aplicable.

Por tanto, al objeto de poder atender correctamente los derechos reconocidos por la LOPD, en base a una buena práctica en relación con el presente Plan de Oficio, se aconseja que por parte de los hospitales, entre otras actuaciones, se elabore un procedimiento escrito en el que se tenga en cuenta la conveniencia de definir una unidad coordinadora para gestión de los derechos ante cualquier solicitud realizada por parte de los afectados que fuera la encargada de centralizar toda la información, informar a todo el personal del hospital sobre cómo actuar ante una solicitud de ejercicio de los derechos de los afectados, estudiar los datos de que se disponga a fin de que se realice una distinción entre los que pueden o no pueden modificarse o cancelarse atendiendo a la diferente legislación estatal y autonómica vigente al respecto, definir los tratamientos de datos que pueden verse afectados por el ejercicio de los derechos de

oposición de los afectados y establecer quién, además del interesado, puede ejercer los derechos y la forma en que debe acreditar su relación con el afectado.

Por otra parte, conforme al artículo 16.3 de la LOPD la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a su supresión.

¤ Entidades de mantenimiento:

Los derechos de los afectados deben atenderse siempre, independientemente de que quien reciba la solicitud disponga o no de sus datos. A estos efectos se recomienda a las citadas entidades la elaboración de procedimientos que permitan el ejercicio efectivo de los derechos.

QUINTA: CREACIÓN, MODIFICACIÓN O SUPRESIÓN DE FICHEROS. NOTIFICACIÓN E INSCRIPCIÓN REGISTRAL.

¤ Laboratorios:

En las inspecciones realizadas se ha detectado que la notificación e inscripción registral de los ficheros de los hospitales no se encuentra actualizada, bien porque se encuentran en fase de revisión o bien porque se encuentran pendientes de la publicación de la correspondiente orden en el Boletín de la Comunidad Autónoma.

Los hospitales de los cuales dependen los laboratorios inspeccionados son de titularidad pública por lo que les es de aplicación el artículo 20 de la LOPD en el que se indica que la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del estado o diario oficial correspondiente.

Por tanto, debe procederse a la publicación actualizada de los ficheros de los hospitales en el diario oficial que corresponda, indicando los siguientes aspectos:

a) La finalidad de los mismos y los usos previstos.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de los datos de carácter personal.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

todo ello a fin de proceder a su inscripción en el Registro General de Protección de Datos.

¤ Entidades de mantenimiento:

En su calidad de prestadores de servicios no están obligados a cumplir con el deber de notificar al Registro General de Protección de Datos los ficheros de los hospitales que pudieran custodiar.

Madrid a 28 de diciembre de 2004

EL DIRECTOR DE LA AGENCIA
ESPAÑOLA DE PROTECCIÓN DE DATOS

Fdo.: José Luis Piñar Mañas