Expediente Nº: E/07559/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas de oficio por la Agencia Española de Protección de Datos ante Osasunbidea, Servicio Navarro de Salud, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 15 de noviembre de 2013, tuvo entrada en esta Agencia un escrito remitido por el Defensor del Pueblo Navarro, con el que traslada una queja planteada en esa Institución frente al Departamento de Salud del Gobierno de Navarra, por tres ciudadanos, por el acceso no autorizado a sus historias clínicas.

Del contenido de su escrito y la documentación aportada por los denunciantes, podría deducirse, que se hubieran producido diversos accesos no autorizados a las historias clínicas de los promotores de la queja, llevados a cabo por un profesional sanitario del Servicio Navarro de Salud-OSASUNBIDEA.

A pesar, de que los hechos ocurridos, suponen posibles infracciones a la LOPD, debido a las fechas en que se produjeron los hechos: 09/05/2006, 21/07/2006 y 28/09/2007, estas se encontrarían actualmente prescritas.

No obstante, el Director de la Agencia ordena la apertura del presente expediente de investigación, en el ejercicio de las potestades de supervisión y control que tiene legalmente atribuidas (ex artículo 37 LOPD), y en orden a la verificación de la adopción por el Servicio Navarro de Salud-OSASUNBIDEA de las medidas necesarias para garantizar el derecho de los pacientes asistidos por dicho Servicio a la salvaguarda y confidencialidad de los datos contenidos en las historias clínicas.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

- Con fechas 16 y 17 de julio de 2014, se realizó visita de inspección en los locales del Servicio de Sistemas de Información Sanitaria dependiente de la Dirección General de Salud, del Departamento de Salud del Gobierno de Navarra, poniéndose de manifiesto, tras las correspondientes comprobaciones, que:

1 La historia clínica de los pacientes del Servicio Navarro de Salud, se gestiona mediante dos aplicativos: uno para Atención Especializada que se denomina **HCI** y otro para Atención Primaria, denominado **ATENEA,** con un total aproximado de 640.000 pacientes.

2 Procedimiento de identificación y autenticación de usuarios con acceso al Sistema de Información de Historias Clínicas: gestión de usuarios:

2.1 El responsable de la Unidad correspondiente solicita al Servicio de Sistemas de la Información el alta del trabajador en el Sistema, bien mediante correo electrónico, aplicación de Avisos Informáticos o envío de

formulario en papel, indicando datos personales y categoría profesional, en el caso de creación de un usuario para Atención Primaria.

2.2 En el caso de que el alta sea solicitado desde Atención Primaria, se dará de alta el usuario con el perfil clínico: médico o enfermera, que aunque tienen acceso a ver la misma información de la historia clínica, los permisos para ciertas acciones, son diferentes, y perfil Administrativo: con acceso a datos identificativos y citaciones.

2.3 Si el alta del usuario es solicitada desde Atención Especializada es absolutamente necesario enviar el formulario en papel, ya que se requiere toda la información que aparece en el mismo para poder asignar usuario.

Para Atención Especializada existen los siguientes perfiles:

Médico

Enfermera

Administrativos

Auxiliares de clínica

Trabajador Social

Farmacéuticos

Otros (Óptico, Fisioterapeuta, Educador, etc.).

No obstante, dichos perfiles no son estancos ya que según el puesto de trabajo que desempeñen se pueden combinar con una serie de permisos, que se pueden añadir o restringir, en su caso.

2.4 En todos los casos, la aplicación genera un correo electrónico que envía al solicitante confirmando el alta del usuario, y se comunica el código de usuario y la contraseña, que son iguales y que el sistema obliga a cambiar en el primer acceso del usuario. Periódicamente es necesario cambiar la contraseña, en el caso de Atención primaria, cada 180 días y en el caso de Atención especializada cada 90 días.

Si el usuario pertenece a Atención Primaria, se le facilita un documento con las normas sobre seguridad, protección de datos y secreto profesional, donde se le informa de que todos los accesos son auditados y unas recomendaciones sobre el uso de la contraseña y del correo electrónico.

2.5 Si el usuario pertenece a Atención Especializada, se le facilita un documento en el que se le informa de diferente normativa Foral y Estatal relativa a confidencialidad y seguridad de la información. En el caso de que un usuario no realice ningún acceso en el periodo de tres meses se pasan a estado inactivo.

2.6 En la actualidad el Servicio Navarro de Salud cuenta con 9555 usuarios activos, aunque no todos ellos cuentan con un perfil que permita el acceso a algún tipo de dato relacionado con la salud y 3007 inactivos, que son los trabajadores que ya no tienen acceso al Sistema de

Información de historias clínicas, pero que es necesario mantenerlos inactivos con el fin de poder realizar investigaciones posteriores a su baja. Los usuarios pasan al estado inactivo a solicitud del responsable de la Unidad o del Departamento de Recursos Humanos.

2.7 En el Acceso inicial al Sistema informático del Gobierno de Navarra, se visualiza un texto donde constan aspectos informativos sobre el uso adecuado de los recursos del Sistema, sean usuarios del ámbito sanitario o no.

2.8 Cuando el usuario accede por vez primera al Sistema de información de historias clínicas se visualiza una pantalla con el siguiente texto: *Todo usuario de esta aplicación está sujeto al secreto profesional, aún en el caso de no ser personal sanitario. No está permitido el uso indebido de la información contenida en esta Base de Datos. Recuerde que su identificación y los accesos que realice quedaran registrados.* También, consta la fecha y hora del último acceso y los intentos fallidos. En dicha pantalla figura un menú en el que, entre otros, existe un enlace con las CONDICIONES DE USO Y CONFIDENCIALIDAD DE HISTORIA CLINICA INFORMATIZADA.

2.9 La contraseña para el acceso al Sistema Corporativo es necesario cambiarla una vez al mes, existe un documento en la red donde se detallan dichas normas, así como la composición de contraseña.

3 Registro de Accesos (auditoria) del Sistema de Información de Historias Clínicas:

3.1 El Sistema registra tanto los accesos como los intentos de acceso fallidos, de estos últimos se registra exclusivamente el código de usuario que intento el acceso. Si el acceso es correcto, se guardan, entre otros, los siguientes datos:

3.1.1 Identificación del usuario,

3.1.2 Fecha y hora inicial del acceso y en el caso de Atención Primaria, también hora de finalización del acceso.

3.1.3 Paciente accedido.

3.2 Si bien, el contenido del Registro de Acceso, se encuentra en periodo de unificación para todo el Sistema Navarro de Salud. Adjuntándose al Acta de Inspección E/7559/2013-I/1, modelos de diseño de Registro de Acceso de Atención Primaria, Atención Especializada y el Unificado que se encuentra pendiente de implantación.

3.3 En la actualidad disponen de información en el Registro de Auditorias desde el año 2000 de todos los datos correspondientes tanto a Atención Especializada como a Atención Primaria.

3.4 Para la consulta a dicho fichero, disponen de un aplicativo que permite el acceso on-line al total de la información contenida en el mismo. Las consultas se realizan por un periodo determinado, en el caso de Atención Primaria por el criterio de código de identificación del paciente y en Atención Especializada por el criterio de historia clínica. También, se pueden auditar los accesos realizados por un usuario determinado.

4 Comité de Auditorias de la Historia Clínica:

4.1 Este órgano colegiado está integrado por representantes de todos los ámbitos asistenciales, por Resolución 3192/2013, de 12 de diciembre, se establece el procedimiento de trabajo de dicho Comité, si bien su creación data del año 2007.

4.2 El Comité realiza auditorias de oficio de accesos a la historia clínica Informatizada, de acuerdo con los protocolos adoptados al efecto, evaluando si los accesos habidos en las historias clínicas de pacientes, han sido presuntamente legítimos o no. Estas auditorías son anuales y se realizan sobre tres colectivos:

4.2.1 Personas de notoria popularidad en la Comunidad Foral.

4.2.2 Personas elegidas de forma aleatoria.

4.2.3 Personas relacionadas con el mundo sanitario.

4.3 El origen de la información utilizada en dichas auditorias, es el Registro de Accesos descrito en el apartado anterior, una vez que se han examinado los accesos seleccionados, se analizan los casos problemáticos y se solicita información adicional a los propios autores de los accesos, las contestaciones son estudiadas por el Comité y, en el caso, que no se consideren procedentes el informe se eleva a los órganos competentes, para que procedan, en su caso, a la incoación de los correspondientes expedientes disciplinarios.

4.4 Una vez finalizadas las actuaciones realizadas por el Comité, se levanta un Acta con las mismas y las conclusiones al respecto.

5 Registro de Incidencias de los Sistemas de Información de historia clínica:

5.1 El Sistema Navarro de Salud cuentan con un aplicativo mediante el cual los usuarios comunican las incidencias que afecten a los datos de carácter personal, así como todo tipo de incidencias en el sistema informático, donde se reflejan los datos del usuario que lo notifica y toda la información relativa a su Resolución. Este aplicativo, es utilizado también, como hemos visto anteriormente, para las solicitudes de altas o bajas de usuarios.

5.2 Por otra parte, el Responsable de Seguridad, dispone de un archivo informatizado, con las solicitudes e incidencias de accesos al Sistema de Información de Historias clínicas, con un promedio de ocho a diez anualmente.

5.3 Se ha verificado que en este Sistema se custodia toda la documentación referente a los expedientes relativos a posibles accesos indebidos en diferentes ocasiones por parte de un médico de Atención Primaria, y que fueron denunciados entre otros, ante el Defensor del Pueblo Navarro, el cual dio traslado a la Agencia Española de Protección de Datos de dichos hechos, dando lugar a las presentes Actuaciones.

5.4 La Ley Foral 17/2010, de 8 de noviembre, de derechos y deberes de las personas en materia de salud en Navarra, en su Capítulo II. *De la confidencialidad*, artículo 31. *Derecho a la confidencialidad de la información*, establece que: …….*El paciente tiene derecho a conocer en todo caso quién ha accedido a sus datos sanitarios, el motivo del acceso*

y el uso que se ha hecho de ellos, salvo en caso del uso codificado de los mismos.

6 Derechos ACCESO RECTIFICACIÓN CANCELACION Y OPOSICIÓN

El Servicio de Atención al Paciente del Sistema Navarro de Salud dispone de un protocolo para dar cumplimiento a los derechos de los pacientes de Acceso, Rectificación, Cancelación y Oposición, para lo cual existe un documento que se pone a disposición de los pacientes, denominado Instancia General.

7 Se verifica la existencia del Documento de Seguridad al que hace referencia el artículo 88 del Real Decreto 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, donde constan las medidas de seguridad establecidas por el Departamento de Salud con relación a la gestión y control de accesos.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

Las presentes Actuaciones Previas de Investigación tiene la finalidad de verificar el cumplimiento de las medidas de seguridad por parte del Servicio Navarro de Salud. El artículo 9 de la LOPD, referente a las medidas de seguridad, dispone lo siguiente:

"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.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

El citado artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, con la finalidad de evitar, entre otros aspectos, el acceso no autorizado por parte de ningún tercero.

Sintetizando las previsiones legales citadas puede afirmarse que:

- Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un

tratamiento sometido a las exigencias de la LOPD.

- Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

- La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se establecen en normas reglamentarias, de modo que se eviten accesos no autorizados.

- El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Reglamento de desarrollo de la LOPD establece que los ficheros que contengan datos de salud deben tener incorporadas las medidas de seguridad de nivel alto.

En el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, en sus tres primeros apartados, se determina lo siguiente:

"1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos."

Las incidencias de seguridad deben quedar reflejadas en dicho documento, como se ha verificado que sucede.

El artículo 103 del citado Real Decreto determina lo referente a los registros de accesos, cuando hay que tener incorporadas las medidas de seguridad de nivel alto, señalando:

"1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad."

Durante la visita de inspección efectuada a Osasunbidea, se verificó que cumplían todo lo señalado en lo referido a las medidas de seguridad establecidas en el Real Decreto 1720/2007.

En consecuencia, se estiman correctas las medidas de seguridad implantadas por parte del Servicio Navarro de Salud.

Las eventuales infracciones derivadas de los accesos indebidos se encuentran prescritas según lo establecido en el artículo 47 de la LOPD.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a OSASUNBIDEA, SERVICIO NAVARRO DE SALUD*.*

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará

conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la LJCA, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos