Sanción AEPD de 200.000 euros sistema de información hospitalaria. Gestión de la Historia Clínica Electrónica. Encargo de tratamiento que no necesariamente implica responsabilidad.

1. Hechos Denunciados.

Un “Ex_trabajador” de HM Hospitales alertó sobre deficiencias de seguridad relacionadas con la gestión de datos personales y el software "Doctoris", el sistema de gestión hospitalaria utilizado por el grupo. Se alegó que las medidas de seguridad no eran suficientes para proteger los datos de los pacientes, incluyendo información sensible como historiales clínicos.

Este software es utilizado por HM en la gestión de la Historia Clínica Electrónica (HCE), y la infraestructura está alojada en los servidores de TRC Informática, empresa encargada del mantenimiento.

El denunciante (ya se tratase de un empleado de HM o del proveedor encargado del mantenimiento del Software) detalló problemas de seguridad relacionados con la gestión de datos sensibles almacenados en el sistema "Doctoris".

2. Incumplimiento.

El incumplimiento consiste en la falta de medidas de seguridad adecuadas, destacando los siguientes puntos:

- Falta de trazabilidad de los accesos a las historias clínicas electrónicas (HCE), lo que impedía identificar a los usuarios que accedían a los registros.

- Carencia de un proceso automatizado para el bloqueo y supresión de datos.

- Cifrado inadecuado de los datos sensibles.

3. Medidas Implementadas por la Empresa.

HM Hospitales defendió que había implementado medidas de seguridad, como:

- Cifrado de las bases de datos y un plan de mejora para migrar a sistemas más robustos.

- Auditorías periódicas para asegurar el cumplimiento normativo.

- Implementación de mecanismos de trazabilidad para los accesos a los datos de los pacientes.

4. Motivación de la Sanción.

La AEPD concluye que:

El sistema no garantizaba una trazabilidad completa de los accesos a los datos de la HCE, salvo en casos de modificación. Esto impedía verificar qué usuarios habían consultado una HCE específica sin realizar modificaciones (es decir, solo a efectos de consultar la HCE)

A pesar de que se contaba con cifrado de datos, el nivel de seguridad inicial era insuficiente, ya que el cifrado se limitaba a los discos duros, pero no a las bases de datos en reposo.

También se detectaron errores en la asignación de perfiles de usuario, permitiendo que personal no autorizado tuviera acceso a datos sensibles.

La resolución hace mención a los fallos cometidos por TRC Informática como encargado del tratamiento, al no garantizar la plena seguridad y trazabilidad en el manejo de los datos en el entorno de "Doctoris" y, pese a ello, no es sancionada ya que **se considera que HM**, **como responsable del tratamiento**, **es quién falla en la obligación de supervisar y verificar que su proveedor implementara las medidas de seguridad adecuadas**. La colaboración de TRC Informática y las mejoras implementadas durante la investigación probablemente influyeron en la decisión de no sancionarla directamente.

La AEPD concluyó que HM Hospitales incumplió el Artículo 32 del RGPD, que exige medidas de seguridad apropiadas. Los motivos principales de la sanción fueron:

Falta de trazabilidad en el acceso a las historias clínicas.

Deficiencias en el bloqueo y eliminación de datos.

Medidas de cifrado insuficientes.

5. Sanción Impuesta.

La AEPD impuso una multa de 200.000 euros a HM Hospitales por la infracción del Artículo 32 del RGPD, tipificada como grave en el artículo 83.4. La multa se basó en la naturaleza de los datos afectados (salud) y las deficiencias en las medidas de protección implementadas.

Resolución sancionadora AEPD https://www.aepd.es/documento/ps-00351-2023.pdf