Capsulas

Los incumplimientos del encargado del tratamiento de datos pueden conllevar sanciones para el promotor del estudio

Resoluciones de la Agencia Española de Protección de Datos de 24 y 25 de febrero de 2025

La protección de los datos personales en el ámbito de la investigación clínica ha cobrado una gran relevancia en los últimos años. La creciente digitalización de los estudios, el uso de soluciones tecnológicas y la intervención de múltiples actores han incrementado tanto la complejidad como el riesgo asociado al tratamiento de datos de salud. En este ámbito, la Agencia Española de Protección de Datos (AEPD) ha emitido dos resoluciones sancionadoras contra una sociedad científica y un grupo de investigadores, respectivamente, por una brecha de seguridad sufrida por un proveedor de servicios de tecnología que prestaba servicios a dichas entidades. De estas resoluciones pueden extraerse algunos aprendizajes prácticos para minimizar el riesgo de sanción en estos casos.

Deficiencias detectadas por la AEPD

Las entidades sancionadas actuaban, en ambos casos, como promotores de un estudio (un registro de pacientes y un estudio observacional). Para gestionar la plataforma en la que se almacenaban los datos de salud, contaban con un proveedor de servicios que actuaba como encargado del tratamiento. La brecha de seguridad consistió en un acceso no autorizado que afectó a los sistemas informáticos del proveedor. La investigación realizada por la AEPD concluyó que el encargado no contaba con las medidas técnicas y organizativas adecuadas, como el cifrado de los datos, para garantizar la seguridad de los datos.

Además, en uno de los casos, la AEPD consideró que existía una deficiente delimitación contractual de los roles de responsable y encargado entre el promotor y los centros participantes, lo que contribuyó a una gestión inadecuada del incidente. Asimismo, la AEPD consideró deficiente la respuesta ante la brecha, ya que la comunicación a los afectados se realizó únicamente a través de la web y a los hospitales y no mediante notificación directa a los participantes.

Responsabilidad proactiva del promotor

En las investigaciones clínicas resulta fundamental aplicar el principio de "privacidad desde el diseño". Esto implica asumir un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva, que incluya la selección de proveedores de servicios que aseguren la protección de la privacidad de los participantes a lo largo de todo el estudio y tras su finalización.

En el caso de los estudios clínicos, esta responsabilidad proactiva corresponde al promotor, que es considerado "responsable del tratamiento" de los datos. En virtud del Reglamento General de Protección de Datos (RGPD) el responsable es quien determina los fines y medios del tratamiento de datos. No obstante, también pueden llegar a ostentar tal condición quienes, aun no siendo promotores, financien el estudio, como sucede en el caso de los llamados "Investigator Initiated Studies", donde a cambio de la financiación pueden llegar a tener acceso a datos personales en el contexto del estudio.

Elección del encargado y medidas de control

La AEPD recuerda que el artículo 28 del RGPD establece que el responsable del tratamiento debe elegir únicamente un encargado que ofrezca

garantías suficientes para aplicar medidas técnicas y organizativas apropiadas al tratamiento que llevará a cabo. La adhesión del encargado a un código de conducta o a un mecanismo de certificación en materia de protección de datos, como sellos y marcas de protección de datos, son elementos que pueden ayudar a demostrar la existencia de estas garantías suficientes.

Dicho artículo también obliga al responsable del tratamiento a establecer contratos adecuados que regulen su relación con el encargado, así como a ejercer un control efectivo sobre las medidas técnicas y organizativas aplicadas por dicho encargado y, en su caso, por los subencargados que éste último pueda a su vez contratar. En consecuencia, según la AEPD, el responsable no puede desentenderse de las actuaciones de sus encargados, sino que debe velar por su buena elección y vigilancia.

De las resoluciones analizadas pueden extraerse otros aprendizajes.

En primer lugar, que cuando un responsable del tratamiento contrata un encargado no es suficiente con firmar cláusulas tipo o confiar en la reputación del proveedor. El deber de diligencia exigible al responsable del tratamiento le obliga a verificar que las medidas adoptadas son adecuadas al riesgo en cada caso, y que se mantienen actualizadas, mediante auditorías y documentación de cumplimiento, verificaciones o checklists periódicos, informes de riesgos, etc.

En segundo lugar, también es importante tener en vigor procedimientos internos para la gestión de las brechas de seguridad, debidamente comunicados y actualizados. Estos procedimientos deben incluir información sobre los canales para comunicar las incidencias y las obligaciones de notificación tanto a AEPD como a los afectados, así como sobre tareas, roles y personas responsables de realizarlas.

°°°°°