La AEPD publica una guía con las claves del sector sanitario

La Agencia Española de Protección de Datos (AEPD) ha publicado recientemente una guía de protección de datos para los profesionales del sector sanitario. Con esta publicación, la AEPD pretende orientar a los profesionales de la salud y facilitar el cumplimiento de la normativa de protección de datos dando respuesta a distintas situaciones que se pueden plantear durante el desarrollo de la actividad en los centros sanitarios.

¿El RGPD conlleva nuevas obligaciones?

Si bien la anterior normativa de protección de datos ya conllevaba estrictas obligaciones para los profesionales sanitarios, el Reglamento General de Protección de Datos conlleva nuevas necesidades:

- La organización deberá realizar una gestión del riesgo de los tratamientos, teniendo en cuenta su naturaleza, el alcance y los fines perseguidos.
- Se deberán aplicar las medidas de seguridad necesarias en función de los riesgos detectados en el análisis anterior.
- Cuando el riesgo detectado sea alto o así lo requiera expresamente la normativa, se deberá realizar una evaluación de impacto (por ejemplo, esta será necesaria cuando se utilicen sistemas de monitorización remota o telediagnóstico).
- Disponer de un registro de actividades del tratamiento correctamente actualizado.
- Nombrar un delegado de protección de datos.

¿Es obligatorio designar un delegado de protección de datos?

La designación de un delegado de protección de datos es obligatoria cuando se trate de centros sanitarios legalmente obligados al mantenimiento de historias clínicas. Por ende, los centros de salud y centros sanitarios (dentistas, centros de estética, centros de fisioterapia, gabinetes de psicología…) han de disponer de un delegado de protección de datos.

¿A qué datos pueden acceder los profesionales sanitarios?

El profesional sanitario y su equipo pueden acceder a la historia clínica del paciente siempre que estén implicados en la asistencia del mismo. Si bien el acceso a las historias clínicas de los pacientes no puede verse restringido cuando sea necesario para la atención eficiente y eficaz del centro (especialmente en los casos de emergencia vital), se debe conservar la información relativa a los accesos a las historias clínicas (quién accedió a la historia clínica, cuándo, etc.) con el ánimo de garantizar que no existan accesos innecesarios para la atención del paciente.

¿Pueden utilizarse los datos del paciente con fines docentes?

El profesional sanitario puede utilizar los datos clínicos del paciente con fines docentes (clases, cursos, ponencias…) siempre que no sea posible identificar al interesado, es decir, que se eliminen previamente los datos identificativos como el nombre, apellidos, direcciones, teléfonos, etc. En caso de que el paciente sea identificable, será necesario recabar su previo consentimiento para esta finalidad.

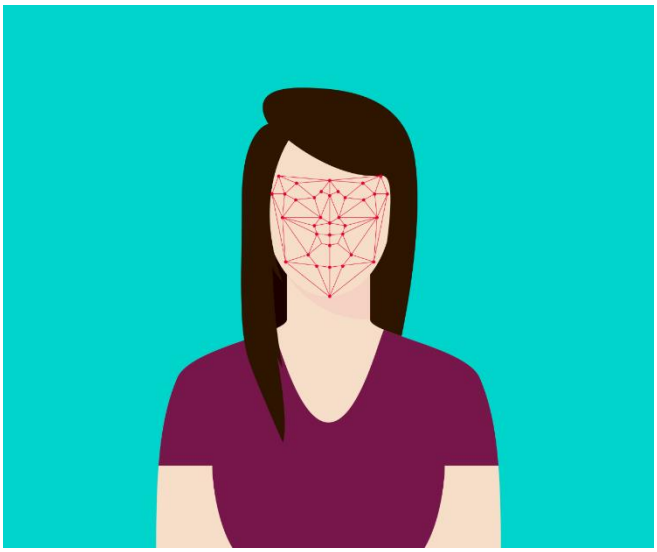
¿Cómo se debe llamar al paciente a consulta?

Con el ánimo de no vulnerar la intimidad de los pacientes, no se les debe llamar a consulta a través de

su nombre y apellidos. Por ello, será necesario utilizar códigos o números asignados a los pacientes para llamarlos a consulta, o en su defecto, utilizar únicamente su nombre de pila.

La Universidad Oberta de Catalunya es sancionada por utilizar el reconocimiento facial con los alumnos

La Universidad Oberta de Catalunya ha resultado sancionada tras la reclamación de un grupo de alumnos, que denunciaron a la entidad por utilizar un sistema de reconocimiento facial. La entidad, que se dedica a la impartición de estudios universitarios a distancia, había implementado un sistema mediante el cual la cámara del alumno registraba las facciones del mismo durante los exámenes, con el ánimo de identificarle inequívocamente y evitar el fraude.



La ACPD (**Autoritat Catalana de Protecció de Dades**) ha sancionado finalmente a la entidad, al entender que no contaba con una base legal suficiente para tratar datos biométricos de los alumnos, es decir, datos relativos a las características físicas de una persona que permiten su identificación única. Cabe destacar que el Reglamento General de Protección de Datos en su artículo noveno prohíbe el tratamiento de esta clase de datos, salvo en determinados supuestos estrictamente tasados.

Esta resolución va en consonancia con el criterio de la Agencia Española de Protección de Datos, que a raíz de la crisis del coronavirus y de la posibilidad de utilizar estos sistemas para evitar el fraude en los exámenes realizados a distancia, estableció que existen sistemas menos intrusivos que permiten hacer frente a la suplantación de identidad en los exámenes a distancia y que, por ende, no vulneran la intimidad de los alumnos.

Finalmente, coinciden las entidades en que el consentimiento otorgado por el alumno para el uso de sistemas de reconocimiento facial no se puede otorgar de forma libre, pues el afectado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

Mi negocio ha sufrido un ataque informático: ¿Qué debo hacer?

El continuo avance de la tecnología ha hecho que la mayoría de los negocios confíen en el entorno digital para conservar la información de sus cuentas, clientes y empleados. Esto conlleva grandes ventajas como la disponibilidad de la información o la flexibilidad de la capacidad disponible, sin embargo, también conlleva riesgos que pueden ocasionar la pérdida de la información de la empresa.

En caso de que sufrir un ataque que conlleve la perdida de disponibilidad, la alteración o la destrucción de la información de un negocio, se deberán seguir los siguientes cinco pasos:

1. Recopilar toda la información disponible del suceso. Se deberá investigar con celeridad para averiguar el origen del incidente. Para ello, se podrá contactar con los empleados implicados o que hayan descubierto el incidente, así como con los proveedores que pudieran verse involucrados.

2. Clasificar la brecha de seguridad. En función de la naturaleza del incidente, se deberá averiguar el tipo de amenaza (si se trata de un fraude, virus, intrusión…) si el ataque ha sido externo o interno, averiguar qué datos se han visto afectados por el incidente, cuál ha sido la ruta o el medio del ataque, etc.

3. Definir el plan de respuesta. Teniendo en cuenta la información disponible del incidente, el responsable de seguridad deberá aplicar las primeras medidas destinadas a la contención del ataque, con el ánimo de limitar los daños causados.

4. Proceso de notificación. Se deberá valorar si existe un riesgo para los derechos de los interesados cuyos datos personales se han visto afectados por el incidente, con la finalidad de determinar si es necesario comunicar este incidente a la autoridad de control o, en su caso, a los propios interesados, como establece la normativa de protección de datos.

5. Estudio de las medidas a adoptar y cierre de la brecha. Con la información obtenida del incidente, se deberán valorar las medidas implementadas para contener, mitigar o eliminar los daños derivados del mismo. Además, se deberá revisar la necesidad de implementar medidas adicionales para evitar que la brecha se repita. Una vez finalizado este proceso, se archivará la brecha de seguridad.

¿Cómo evitar que mi negocio sufra una violación de la seguridad?

La ciberseguridad es una labor que, para ser efectiva, debe mantenerse en el tiempo, actualizarse y revisarse con periodicidad. No obstante, la aplicación de medidas de seguridad desde el diseño y por defecto sí pueden ayudar a prevenir la mayoría de los ataques. Los aspectos a tener en cuenta deben ser los siguientes:

i. Analiza los riesgos antes de implementar nuevos tratamientos. Es necesario que, antes de comenzar con un nuevo proyecto o tratamiento, se analicen los riesgos que puedan derivar del mismo con la finalidad de aplicar las medidas de seguridad necesarias para garantizar la seguridad en función del riesgo detectado. De esta manera, el diseño del nuevo proyecto deberá tener en cuenta la seguridad de la información.

ii. Cuenta siempre con copias de seguridad. Es necesario que cualquier negocio se dote de una copia de seguridad fuera de los locales (como, por ejemplo, un back up online) y otra copia dentro de las propias instalaciones. De esta manera, se puede asegurar que, aunque falle una de las dos copias, se dispone de la otra para recuperar la información.

iii. Forma a los empleados. Es inútil gastar miles de euros en recursos informáticos y medidas de seguridad si las personas que tratan la información a diario no son conocedoras de sus obligaciones en materia de seguridad. Es necesario que el personal con acceso a datos conozca sus obligaciones y tengan unas instrucciones claras en materia de seguridad.

Editado por Microlab Hard

Madrid. C/ Cronos 8, 1º, Madrid

Barcelona. C/ Santiago Rusiñol 8, Molins de Rei