Datos de Salud y Protección de Datos Personales

¿Qué son datos personales relacionados con la salud?

Es aquella información **concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona**, incluyendo la información que se derive de un acto médico, el grado de discapacidad y su información genética.
Con la entrada en vigencia del nuevo Reglamento de Protección de Datos, los datos neuronales también son datos protegidos.

¿Qué marco regulatorio es aplicable para resguardar dichos datos personales?

La Ley de Protección de Datos Personales (Ley N° 29733), su Reglamento vigente (Decreto Supremo N° 003-2013-JUS), y su nuevo Reglamento (Decreto Supremo N° 016-2024-JUS) establecen un marco normativo que resguarda la confidencialidad, accesibilidad y disponibilidad de los datos personales relacionados con la salud, las multas actualmente pueden llegar hasta las 50 UIT, y con la aplicación del nuevo Reglamento hasta las 100 UIT.

Sumado a ello, teniendo en cuenta la sensibilidad de la información que contiene todo acto médico, el MINSA emitió en el 2020 una Directiva (Directiva Administrativa N° 294-MINSA/2020/OGTI), la cual establece parámetros para el tratamiento de datos personales relacionados con la salud (en adelante, “DPS”), la cual estable lo siguiente:

- Los DPS se generan en todo acto médico o acto en salud, o cualquier atención de salud que se reciba en un establecimiento de salud o fuera de él, incluyendo los servicios de telemedicina.
- Los DPS no pueden ser difundidos, ni tratados de manera que se vulnere la debida reserva y confidencialidad de éstos.
- Se requiere obtener necesariamente el consentimiento por escrito del titular; salvos lo casos autorizados por ley lo autorice, siempre que atienda a motivos de interés público, salud pública y en casos de circunstancias de riesgo para el titular de los DPS, siempre que dicho tratamiento sea realizado en los establecimientos de salud o por profesionales de la salud, respetando el secreto profesional.
- Los titulares de los DPS pueden ejercer sus derechos de acceso, rectificación, cancelación u oposición (ARCO) al tratamiento de sus datos personales sensibles, conforme a la Ley de Protección de Datos Personales.
- El personal asistencial y administrativo es responsable del respeto a la reserva y privacidad de las personas atendidas.
- Los DPS solo podrán salir del establecimiento de salud (EESS) o servicio médico de apoyo (SMA) en los casos contemplados por la ley, o con el consentimiento del titular de los DPS, o si se trata de datos anonimizados
- Se debe designar a personal que implemente las medidas de seguridad técnicas, organizativas y legales para protección de los DPS, evitando la pérdida o destrucción de esto, tanto en forma manual como a través del uso de las TICs.
- Se establecen criterios de confidencialidad y un anexo de confidencialidad a ser suscrito por empleados y terceros.

En ese sentido, el deber de confidencialidad de información contenida en actos médicos también está respaldada en normativa especial, y la infracción al indicado deber de confidencialidad genera, entonces, contingencias importantes para los responsables del tratamiento de dichos datos personales, los cuáles van desde multas administrativas, hasta acciones civiles.

Recordemos que los establecimientos de salud son considerados activos críticos nacionales, por lo que al día de hoy, cualquier filtración de datos se sujeta al D.U. 007-2020, por lo que existe la obligación de notificar el incidente.

Multas a empresas que no han aplicado medidas de seguridad sobre datos sensibles

Resolución Directoral 3023-2022-JUS/DGTAIPD-DPDP	El establecimiento de salud incumplió con adoptar las siguientes medidas de seguridad: (i) No documentar los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados; (ii) No generar ni mantener registros de interacción lógica de su servidor, (iii) No evidenciar la implementación de medidas de seguridad perimetrales del ambiente en el que se encuentra ubicado el servidor de datos; (iv) No garantizar el respaldo del banco de datos personales de pacientes, (v) No contar con controles para la generación de copias o reproducción de documentos. Multa impuesta: 9.28 UITs

Resolución Directoral 1436-2021-JUS/DGTAIPD-DPDP	Se sancionó al haber realizado tratamiento de datos personales incumpliendo la obligación de confidencialidad al haber transferido los datos del denunciante (información médica) sin que éste haya otorgado su consentimiento para dicho tratamiento. Multa impuesta: 18 UITs
Resolución Directoral 4037-2022-JUS/DGTAIPD-DPDP	El establecimiento de salud habría dado acceso a la historia clínica de la denunciante por parte de un tercero no autorizado, con una omisión relevante respecto de la autorización de la denunciante y la mención y evaluación del motivo de la solicitud de dicha información de salud. Multa impuesta: 30 UITs

RECOMENDACIONES

¿Qué medidas de seguridad debemos aplicar?

- Capacitar constantemente en protección de datos personales y seguridad de la información al personal clave.
- Incluir dentro de las faltas al incumplimiento de las medidas de seguridad y al deber de confidencialidad.
- Contar con registro de control de accesos y privilegios en los sistemas donde están contenidos los datos personales.
- Realizar una revisión periódica de las medidas de seguridad.
- Contar con registros que provean evidencia de las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad.
- Implementar medidas de seguridad que impidan al personal no autorizado la generación de copias o la reproducción de documentos digitales que contengan datos personales.
- Verificar que todo el personal clave cuente con cláusulas de protección de datos personales y de confidencialidad en sus contratos.

Material preparado por el área de Protección de Datos Personales y Seguridad de la Información.

Para más información, contactarse a los siguientes correos electrónicos:

- carolquiroz@esola.com.pe
- danielachavez@esola.com.pe

ESTUDIO OLAECHEA

Estudio Olaechea
Estudio Olaechea
www.esola.com.pe

Carol Quiroz
Socia

Daniela Chávez
Asociada