H · D LEGAL

HDGROUP.CL

Alerta Legal

Protección de Datos Personales, Ciberseguridad y Nuevas Tecnologías

Mayo 2025

NORMA TÉCNICA N°241 DEL MINISTERIO DE SALUD: PROCEDIMIENTO DE ANONIMIZACIÓN DE DATOS ABIERTOS EN SALUD

+56 2 2405 3200
AV. VITACURA 2939 – 8TH FLOOR
LAS CONDES, SANTIAGO, CHILE

H · D LEGAL

El Ministerio de Salud aprobó la **Norma Técnica N°241** mediante el Decreto Exento N°23 (30 de abril de 2025), estableciendo nuevas reglas para garantizar la anonimización de datos estructurados antes de su publicación como datos abiertos. Esta alerta legal presenta los principales aspectos de la norma, incluyendo su propósito, técnicas exigidas, procedimiento, implicancias y recomendaciones clave para su implementación por parte de instituciones del sector salud.

I. Principales aspectos de la Norma Técnica N°241

1.1. Finalidad y Alcance

La Norma Técnica N°241 establece los lineamientos obligatorios que deben seguir las instituciones del sector salud para **anonimizar datos estructurados** antes de su publicación como datos abiertos. Su objetivo es compatibilizar el deber de transparencia con la protección de los datos personales, en especial los de carácter sensible.

Aplica a todas las entidades relacionadas con el MINSAL (Subsecretarías, Servicios de Salud, SEREMI, establecimientos).

La norma excluye expresamente aquellos datos no estructurados (como texto libre, imágenes, audio) y bases utilizadas para fines clínicos o de vigilancia epidemiológica.

1.2. Fundamentos y Principios

La norma se basa en lo dispuesto por la Ley Nº 19.628 sobre protección de la vida privada (recientemente modificada a través de la Ley Nº 21.719) y en recomendaciones del Consejo para la Transparencia (Oficio E7986/2022). Adopta principios claves como (1) minimización de datos, (2) prevención de reidentificación y (3) seguridad de la información, articulando así un estándar sectorial para la protección de datos personales en el contexto de responsabilidad de la institución pública que trata datos personales.

1.3. Técnicas y Estándares de Anonimización

La norma exige aplicar técnicas como **supresión**, **generalización**, **perturbación de datos** y **ofuscamiento**, todas orientadas a evitar que una persona pueda ser identificada directa o indirectamente a partir de los datos

publicados. Además, establece el cumplimiento mínimo de dos medidas clave: la **k-anonimidad**, que requiere que cada registro sea indistinguible de al menos otro, y la **l-diversidad**, que busca que dentro de cada grupo de datos similares exista variedad en los valores de información sensible (como diagnósticos), evitando así que se pueda deducir algo personal con certeza.

1.4. Clasificación de Variables

Uno de los primeros pasos del proceso consiste en clasificar correctamente las variables contenidas en la base de datos.

La norma establece cuatro tipos:

- Primero, los **identificadores explícitos**, como el nombre, el RUN o el correo electrónico, que permiten reconocer directamente a una persona. Estos deben ser eliminados por completo.

- Luego, están los **cuasi-identificadores**, como la edad, el sexo o la comuna de residencia. Aunque no identifican por sí solos, podrían hacerlo si se combinan con otros datos, por lo que deben ser transformados para reducir ese riesgo.

- En tercer lugar, se encuentran los **atributos sensibles**, como el estado de salud, la pertenencia a un grupo étnico o las creencias religiosas, que por su naturaleza requieren un nivel de protección más alto.

- Por último, están los **atributos no sensibles**, que no exponen aspectos privados ni permiten identificar a una persona. Estos pueden mantenerse en la base si no implican riesgos de reidentificación.

1.5. Procedimiento y Validación

El proceso establecido por la norma contempla, en primer lugar, la clasificación de las variables contenidas en la base de datos según su naturaleza (identificadores, cuasi-identificadores, atributos sensibles o no sensibles). Luego, se deben aplicar las técnicas de anonimización correspondientes, conforme al tipo de dato y al nivel de riesgo que presentan. Posteriormente, la base debe ser sometida a una verificación técnica, que incluye el análisis de anonimización alcanzada y la realización de la "*prueba del intruso motivado*" para evaluar el riesgo de reidentificación. Finalmente, se exige una validación formal del proceso, que debe quedar documentada

mediante el formulario institucional definido en la norma y una consulta técnica al Departamento de Estadísticas e Información de Salud (DEIS) del MINSAL.

1.6. Herramientas, Roles y Seguridad

La norma recomienda herramientas como ARX o programación en R, sin limitar su uso exclusivo. Define responsabilidades tanto para las jefaturas como para los equipos técnicos y exige documentar el proceso completo. Se requiere también mantener medidas de seguridad posteriores a la publicación, con auditorías y reevaluaciones periódicas frente a nuevas amenazas de reidentificación.

II. Implicancias prácticas para las instituciones públicas del sector salud

La entrada en vigencia de la Norma Técnica N°241 implica cambios operativos relevantes para todas las entidades públicas del sector salud que publiquen datos abiertos con información de personas. Su aplicación requiere integrar nuevas prácticas de tratamiento de datos personales, alineadas con estándares técnicos de anonimización que hasta ahora no estaban formalmente regulados a este nivel.

Entre los principales efectos prácticos de la norma, se pueden presentar:

- **Revisión de protocolos internos**: Será necesario actualizar políticas de publicación de datos, incorporando procedimientos de anonimización compatibles con la norma.

- **Asignación de roles formales**: La norma exige identificar responsables y equipos técnicos encargados del proceso, lo que implica una reorganización de tareas y definición de perfiles.

- **Evaluación de bases de datos activas y futuras**: Las instituciones deberán identificar qué conjuntos de datos requieren anonimización antes de ser difundidos.

- **Ajustes en tiempos, recursos y capacidades técnicas**: El proceso de anonimización (incluyendo validación y revisión) puede requerir nueva infraestructura o capacitación especializada.

- **Cumplimiento normativo y prevención de riesgos**: Aplicar el procedimiento según lo instruido servirá como respaldo ante eventuales cuestionamientos legales por exposición indebida de información personal.

En conjunto, la norma eleva el estándar en la gestión de datos abiertos en salud, fortaleciendo la transparencia responsable, pero también exige un esfuerzo institucional sostenido para cumplir con sus exigencias técnicas y operativas.

III. Recomendaciones para su implementación

La correcta aplicación de la Norma Técnica N°241 requiere que las instituciones públicas del sector salud incorporen prácticas nuevas en el tratamiento de datos personales. A modo general, se sugiere:

- **Actualizar reglamentos y manuales internos**, incorporando procedimientos de anonimización conforme a los lineamientos técnicos establecidos por la norma.
- **Designar formalmente responsables del proceso**, tanto desde la jefatura institucional como en el plano técnico-operativo.
- **Capacitar a los equipos clave** en conceptos como k-anonimidad, l-diversidad y uso de herramientas como ARX o R.
- **Identificar y priorizar datasets (conjunto de datos) sensibles** que puedan ser publicados, evaluando su riesgo de reidentificación.
- **Documentar cada proceso de anonimización**, utilizando el formulario oficial de la norma como respaldo para auditorías y revisiones.

Estas acciones permitirán cumplir con las obligaciones normativas, reducir los riesgos legales asociados a la publicación de datos personales y fortalecer la gobernanza institucional de la información.

IV. Vigencia

La Norma Técnica N°241 rige desde la fecha de su aprobación mediante el **Decreto Exento N°23 del 30 de abril de 2025**, siendo **obligatoria de inmediato** para todas las entidades del sector salud que publiquen datos abiertos. No se contempla un período de transición.

Para más información, contactar a:

Juan Pablo González
Director
Protección de Datos Personales, Ciberseguridad y Nuevas Tecnologías
jpgonzalez@hdgroup.cl

Valentina Palma
Asociada Senior
Protección de Datos Personales, Ciberseguridad y Nuevas Tecnologías
vpalma@hdgroup.cl