

Legal |
Opinión | Artículo 1 de 1

¿Quién administra realmente la información clínica de los pacientes?

"...La entrada en vigencia de la nueva Ley de Protección de Datos Personales representa uno de los cambios regulatorios más importantes para el sector salud en las últimas décadas. Sin embargo, reducir su impacto a una obligación de fortalecer la ciberseguridad o actualizar políticas de privacidad sería un error. Lo que está en juego es mucho más profundo: la forma en que las clínicas deberán administrar uno de sus activos más sensibles y, al mismo tiempo, uno de los derechos más relevantes de las personas..."

Lunes, 20 de julio de 2026 a las 11:30



A⁻ A⁺ Imprimir Enviar

Marcelo Gallardo

En diciembre pasado, un grupo de *hackers* vulneró los sistemas de un prestador de salud privado en Chile y sustrajo cerca de 250 GB de información: fichas clínicas completas, resultados de exámenes de alta sensibilidad — incluyendo diagnósticos de VIH— y copias de cédulas de identidad de pacientes. Meses después, parte de esa información terminó publicada en la *dark web*. El episodio, lejos de ser aislado, se sumó a una alerta emitida este año por la autoridad de ciberseguridad del Estado a todo el sector salud, advirtiendo que el riesgo de filtración de historiales clínicos electrónicos es "latente" para el sistema en su conjunto. Ese antecedente no es anecdótico: es la mejor demostración de que la pregunta sobre quién administra realmente la información clínica de los pacientes dejó de ser teórica.

La entrada en vigencia de la nueva Ley de Protección de Datos Personales representa uno de los cambios regulatorios más importantes para el sector salud en las últimas décadas. Sin embargo, reducir su impacto a una obligación de fortalecer la ciberseguridad o actualizar políticas de privacidad sería un error. Lo que está en juego es mucho más profundo: la forma en que las clínicas deberán administrar uno de sus activos más sensibles y, al mismo tiempo, uno de los derechos más relevantes de las personas.

Cada día, los prestadores privados reciben y procesan enormes volúmenes de información clínica. Fichas médicas, resultados de exámenes, imágenes diagnósticas, antecedentes de hospitalizaciones, tratamientos, intervenciones quirúrgicas y múltiples datos que permiten reconstruir la historia de salud de una persona. La nueva ley reconoce expresamente que esta información constituye una categoría de datos sensibles, sometida a un estándar reforzado de protección, confidencialidad y tratamiento.

Ello obliga a las clínicas a revisar mucho más que sus sistemas informáticos. La protección de los datos clínicos pasa a convertirse en una materia de gobierno corporativo, gestión de riesgos y *compliance*. Será indispensable revisar los protocolos internos, redefinir los perfiles de acceso a la información, establecer mecanismos de trazabilidad, regular adecuadamente los consentimientos para el tratamiento de datos y contar con procedimientos eficaces para responder ante eventuales incidentes de seguridad. La nueva normativa exige, además, notificar las brechas de seguridad a la autoridad dentro de un plazo de 72 horas desde su detección y sin dilación indebida a los titulares afectados cuando exista un riesgo alto para sus derechos, lo que obliga a las organizaciones y a los prestadores de salud, en particular, a contar con procesos previamente diseñados y equipos preparados para reaccionar oportunamente dentro de ese plazo, más que a improvisar una respuesta una vez ocurrido el incidente.

Quizás el mayor desafío no será tecnológico, sino organizacional. Una parte importante de los riesgos asociados a la información clínica proviene del acceso cotidiano que médicos, profesionales de la salud y personal administrativo tienen a datos altamente sensibles. Por ello, las clínicas deberán fortalecer las obligaciones de confidencialidad, capacitar permanentemente a sus trabajadores, establecer controles efectivos sobre acceso y uso de la información y definir claramente las responsabilidades laborales derivadas de un eventual uso indebido de los antecedentes clínicos. La responsabilidad frente al paciente siempre recaerá sobre la institución que decide cómo esa información es recopilada, utilizada y protegida.

A este nuevo escenario se suma otro desafío regulatorio igualmente relevante. Las clínicas no solo deberán cumplir con las obligaciones derivadas de la nueva Ley de Protección de Datos Personales, sino también con aquellas establecidas en la Ley sobre Derechos y Deberes de los Pacientes, toda vez que a ello se agrega el proyecto de ley actualmente en trámite en el Congreso (Mensaje N° 344-372), que fortalece a la Superintendencia de Salud y amplía las atribuciones de la Intendencia de Prestadores: entre otras facultades, le permitirá exigir a los prestadores institucionales el acceso a antecedentes clínicos en el marco de auditorías clínicas o resolución de reclamos, con la obligación expresa de resguardar su condición de dato sensible. De aprobarse, esto significa que la protección de los datos clínicos no solo dependerá del prestador y de la futura Agencia de Protección de Datos Personales, sino que quedará también bajo la mirada directa de un regulador sectorial con facultades sancionatorias reforzadas.

En consecuencia, las clínicas deberán prepararse para un escenario en el que la protección de los datos clínicos dejará de ser una obligación exclusivamente sanitaria para transformarse en una materia sometida a distintos mecanismos de supervisión, con exigencias cada vez más elevadas en materia de seguridad, trazabilidad y responsabilidad institucional.

Pero quizás el cambio más interesante no sea el aumento de las obligaciones para las clínicas, sino el fortalecimiento de los derechos de los pacientes. La convergencia entre la nueva legislación sobre protección de datos personales y la evolución de la regulación sanitaria parece apuntar hacia un modelo en el que las personas ejercerán un control mucho más efectivo sobre su información clínica. Si ese proceso se consolida, Chile podría avanzar progresivamente hacia una verdadera portabilidad de los antecedentes

clínicos, permitiendo que el paciente —y no las distintas instituciones donde ha sido atendido— sea quien decida, mediante los consentimientos correspondientes, cómo compartir su información entre prestadores y autoridades cuando ello resulte necesario para garantizar una mejor continuidad asistencial.

Más que una reforma tecnológica, estamos frente a un cambio de paradigma. La protección de los datos clínicos deja de ser una cuestión meramente documental para convertirse en un elemento esencial de la calidad de la atención, de la confianza de los pacientes y del cumplimiento regulatorio de las instituciones de salud. Las clínicas que comprendan tempranamente esta transformación no solo estarán mejor preparadas para enfrentar el nuevo marco normativo; también estarán contribuyendo a construir un sistema de salud más seguro, más transparente y, sobre todo, más centrado en la protección de los derechos de las personas.

EL MERCURIO

Términos y condiciones de la Información © 2002 El Mercurio Online