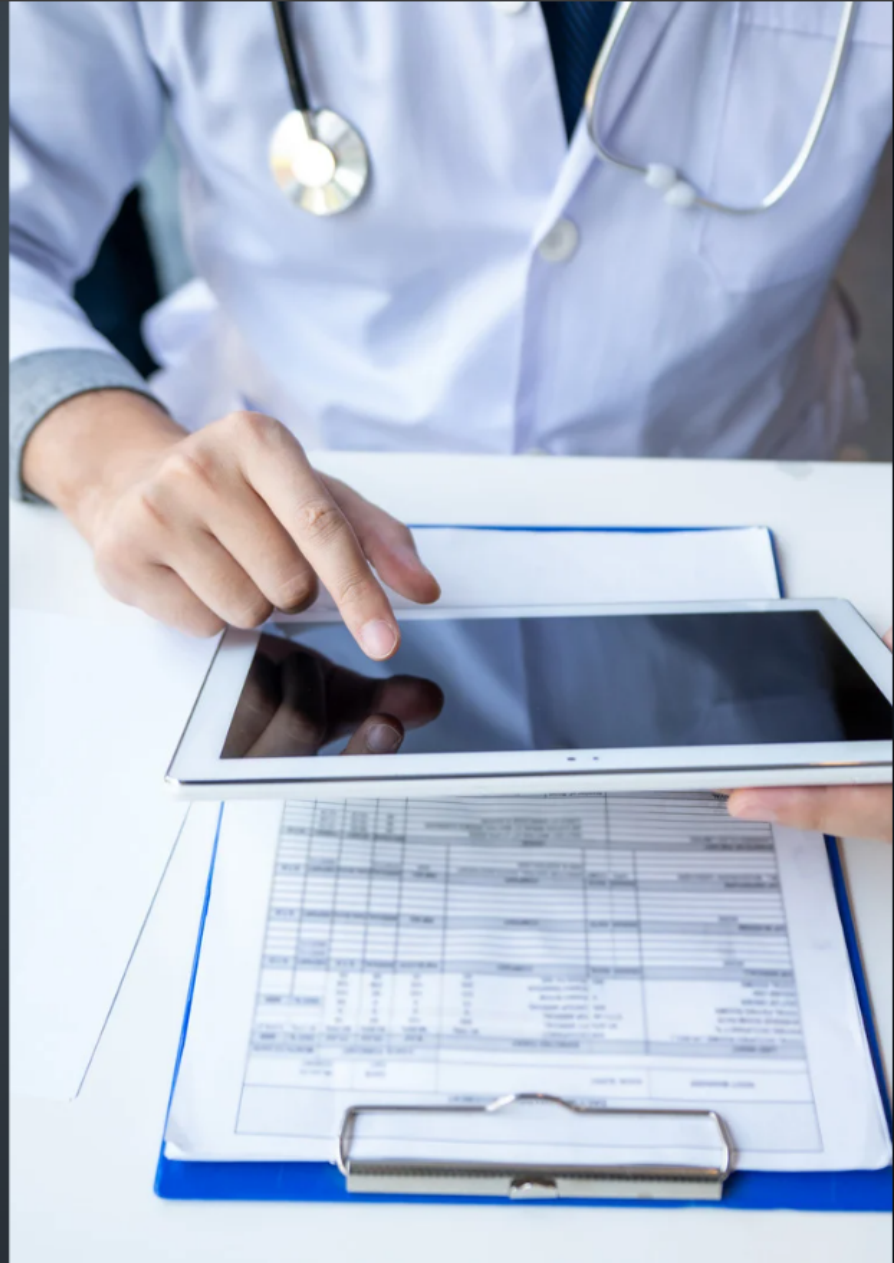
Más allá de los sistemas: protección de datos médicos en entornos físicos y digitales

Magister Nicole Angel Sánchez Rojas



¿Por qué hablar de esto hoy?

- La información médica es uno de los tipos de datos más sensibles.
- Un error, una filtración, una “conversación inocente” puede tener consecuencias graves.
- Casos recientes han puesto en evidencia que la vulneración de datos médicos no solo es técnica, también es humana.
- Objetivo: Entender riesgos, responsabilidades y cómo proteger mejor la información de nuestros pacientes.

Datos sensibles personales

Revelan información sobre aspectos más íntimos o privados de una persona.

Datos sobre:

- Salud
- Origen étnico o racial,
- Creencias religiosas
- Opiniones políticas,
- Orientación sexual,
- Antecedentes penales, etc.

¿Qué son los datos sensibles en salud?

Datos que revelan estado de salud, historial médico, diagnósticos, tratamientos, discapacidades, VIH, salud mental, salud sexual, entre otros.

Tienen protección reforzada por ley.

Su uso o divulgación indebida puede vulnerar derechos fundamentales.

PROCESAMIENTO DE DATOS

Datos

Información

conocimiento

Conceptos Generales

Datos

Son unidades de información no procesada, cuando pasan por cierto proceso se conviernten en información específica y esta información puede convertirse en conocimiento

Algoritmos

Es una secuencia de instrucciones bien definida que se utiliza para resolver un problema o realizar una tarea, fundamentales para el procesamiento de datos y obtener un resultado

Procesamiento de datos

Es la coinversión de datos a información y de información a conocimiento a través de algoritmos y procedimientos computacionales.

¿Cúando se vulneran datos?

- 📂 Expedientes visibles o mal archivados.
- 🗣️ Comentarios en pasillos, ascensores o redes sociales.
- 📸 Fotografías de fichas o pacientes sin consentimiento.
- 📰 Filtraciones a medios (casos de embarazos, VIH, adicciones).
- 💻 Accesos no autorizados al sistema.

Amenazas multifacéticas a la confidencialidad y los datos

Dimensiones de la vulneración de datos

- Ciberataques sofisticados: la amenaza digital en constante evolución.
- Filtraciones internas: el riesgo del acceso indebido por personal autorizado.
- Divulgaciones públicas: exposición en medios de comunicación y redes sociales.
- Acceso físico no autorizado: vulnerabilidades en entornos clínicos.
- Datos de figuras públicas: desafíos adicionales en la gestión de la privacidad.

Riesgos legales y éticos de la vulneración

La exposición de datos médicos sensibles conlleva graves implicaciones.

Impacto en la confianza del paciente

Erosión de la relación médico-paciente y desconfianza en el sistema de salud.

Sanciones regulatorias

Multas elevadas y penalizaciones por incumplimiento de normativas de protección de datos.

Daño reputacional

Pérdida de prestigio para profesionales y organizaciones de salud.

Demandas legales

Posibles acciones civiles por daños y perjuicios a los afectados.

Casos reales e implicaciones

📰 **Prensa publica historia clínica de una figura pública.**
→ Violación del secreto profesional, daño moral, sanción al centro.

📸 **Foto de paciente compartida en grupo de WhatsApp del hospital.**
→ Sanción interna + denuncia por daño a la imagen.

📂 **Médico que se lleva copias de historias clínicas.**
→ Incumplimiento grave, riesgo de fuga de datos.

Casos reales e implicaciones

📁 **Sistema de registro sin restricciones: prensa accede a datos de pacientes tras accidente colectivo.**

→ Se publica información médica sin consentimiento (nombres, diagnósticos, evolución), vulnerando la privacidad de heridos y fallecidos.

→ Implicaciones legales por omisión de medidas de seguridad, revictimización de pacientes y familiares.

Algoritmo analiza historiales médicos sin anonimización ni consentimiento.

→ Hospital implementa sistema de IA para detectar patrones en diagnósticos, pero utiliza datos reales sin encriptar ni consentimiento previo.

→ Riesgo de sesgos, filtraciones, identificación indirecta de pacientes.

→ Posible vulneración del principio de minimización, seguridad y finalidad en el tratamiento de datos sensibles.

Marco jurídico aplicable: Pilares de la protección

Secreto profesional

Base ética y legal que obliga a los profesionales a guardar la confidencialidad.

Leyes de protección de datos

Normativas como el RGPD que establecen un marco estricto para el tratamiento de datos personales.

Limitaciones por interés público

Excepciones que permiten la divulgación bajo circunstancias muy específicas y justificadas.

Responsabilidades legales ante incidentes de seguridad

Profesionales de la salud

- Cumplimiento del secreto profesional y la normativa de protección de datos.
- Obligación de notificar incidentes de seguridad a las autoridades competentes.
- Responsabilidad individual ante negligencia o dolo en la gestión de la información.

Estrategias de prevención integral

- 🗣️ Evitar hablar de pacientes en espacios comunes o redes sociales o a través de medios inseguros como whatsapp.
- 🗂️ Cuidar el acceso y almacenamiento de historias clínicas físicas y digitales.
- 🔐 Usar contraseñas seguras y no compartirlas.
- 📄 No divulgar diagnósticos sin consentimiento del paciente.
- 🧑‍⚕️ Participar en capacitaciones periódicas sobre confidencialidad.

Conclusiones
La privacidad también salva vidas

Proteger los datos médicos no es un trámite legal, es una muestra de respeto y humanidad.

Cada acción cuenta: desde cómo archivas, hasta cómo hablas.

Confianza, dignidad y ética: tres razones por las que esto sí importa.

La confidencialidad no se terceriza. Es una responsabilidad de todos.

Más allá de los sistemas: protección de datos médicos en entornos físicos y digitales

DATOS DE CONTACTO:

Linkt.ree

CORREO: niicolesanchez44@gmail.com

LINKEDIN: https://www.linkedin.com/in/nicole-angel-sanchez-rojas-44nasr/

IG: niicolesanchez44