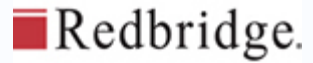


Entrenamiento de HIPAA

Dr Carlos Fernandez DNP, FNP-BC, PMHNP-BC

Director of Case management Department & **Oficial de Cumplimiento de HIPAA**

HIPAA: Ley de Portabilidad y Responsabilidad del Seguro Médico



Enfoque práctico para proteger PHI/ePHI y prevenir violaciones.

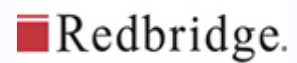


Protección de la información de salud en el entorno sanitario



Guía práctica para el cumplimiento en clínica y comunidad

Objetivo general del módulo



Comprender la normativa HIPAA y su propósito



Proteger PHI y ePHI en la práctica diaria



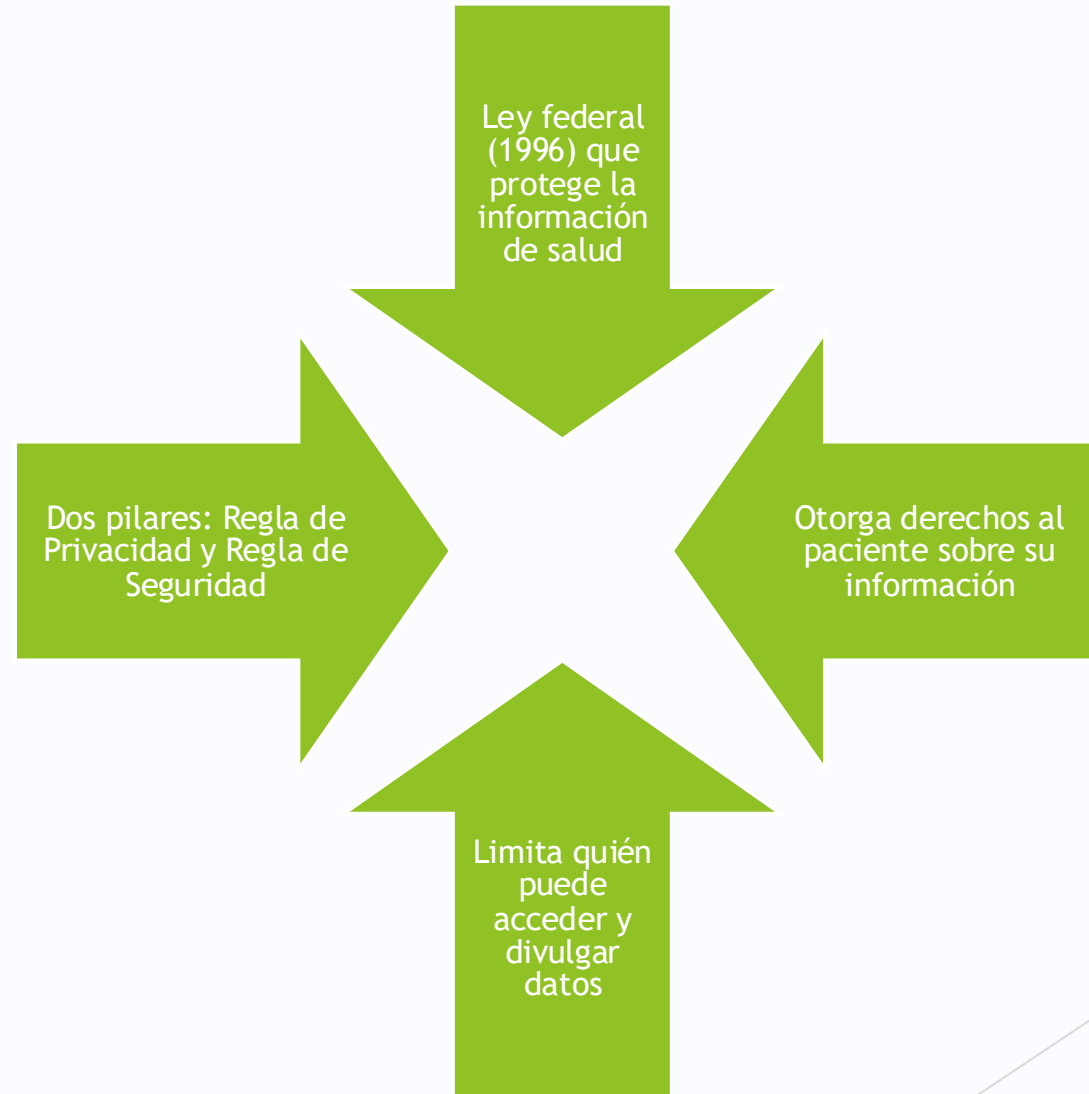
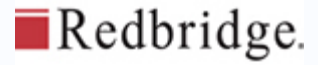
Aplicar medidas de privacidad y seguridad



Prevenir, identificar y reportar violaciones

43_PCABP-00077

¿Qué es HIPAA?



43_PCABP-00077

¿Cual es el objetivo de HIPAA?

Redbridge.

El **objetivo de HIPAA** es **proteger la información de salud privada de los pacientes** mientras permite que la información médica fluya cuando sea necesario para brindar atención, pagar por ella y asegurar la calidad del cuidado.

Establece reglas para:

- **Privacidad** – mantener la información del paciente confidencial.
- **Seguridad** – proteger la información de salud electrónica contra accesos no autorizados.
- **Derechos del paciente** – permitir que los pacientes vean y controlen su propia información médica.

En resumen, se trata de **mantener la información de salud segura, privada y accesible solo para las personas autorizadas.**

43_PCABP-00077

¿La ley HIPAA aplica a nivel internacional?

■ Redbridge.

HIPAA no es una ley internacional general de privacidad. Sin embargo, no es dónde está ubicada la empresa, sus empleados o sus servidores, sino si la organización cumple con la definición de “Covered Entity” (Entidad Cubierta) o “Business Associate” (Asociado de Negocios) según HIPAA, incluso cuando la información médica protegida se crea, accede, procesa o almacena fuera de los Estados Unidos, como parte de sus funciones reguladas.

Planes de salud en EE. UU., como El Plan de Beneficios del Área Canalera, es una “Covered Entity”. Los “Business Associates” incluyen Proveedores, consultores o empresas de servicio que crean, reciben, mantienen o transmiten información médica protegida (PHI) para una Covered Entity, como Redbridge.

43_PCABP-00077

¿La ley HIPAA aplica a nivel internacional?

■ Redbridge.

Una empresa fuera de Estados Unidos también puede ser considerada Business Associate si realiza estas funciones para una Covered Entity o para otro Business Associate.

Cumplir con HIPAA no reemplaza las leyes de privacidad o salud en Panama. Pero las organizaciones que manejan información médica entre países normalmente deben cumplir con HIPAA en la medida en que la ley lo permita

Regla de Privacidad de HIPAA (Privacy Rule)

 Redbridge.

Aplica a PHI oral, escrita y electrónica
Limita uso y divulgación sin autorización
Exige confidencialidad y mínimo necesario
Protege derechos del paciente

Regla de Seguridad de HIPAA (Security Rule)

 Redbridge.

Aplica a ePHI (PHI en formato electrónico)

Requiere salvaguardas administrativas, físicas y técnicas

Control de acceso, auditoría y protección de transmisión

Cifrado/encryptación cuando sea apropiado

■ Redbridge.

Información que identifica a una persona y se relaciona con su salud

Incluye diagnósticos, tratamientos, resultados, facturación

Contiene identificadores (ej. nombre, fecha de nacimiento, MRN)

Debe destruirse adecuadamente (p. ej., triturar)

■ Redbridge.

Registros clínicos electrónicos, portales, facturación online

Calendarios de citas y bases de datos

Laptops/tablets/USB con datos

Videos/fotos digitales con información del paciente

■ Redbridge.

IIHI: información individual identificable (demografía, SSN, email, zip)

PTO: Pago, Tratamiento y Operaciones

Entidad cubierta: organizaciones/personas con acceso a PHI

OCR: Oficina de Derechos Civiles (HHS)

Roles obligatorios: Oficial de Privacidad y de Seguridad

 Redbridge.

Oficial de Privacidad: políticas, entrenamiento, investigación y reporte

Oficial de Seguridad: medidas para proteger ePHI y cumplir Security Rule

Ambos son puntos de contacto ante incidentes.

Redbridge tiene su official de cumplimiento de HIPAA(Dr Carlos Fernandez
email cfernandez@redbridge.cc)

■ Redbridge.

Business Associate: tercero con acceso a PHI/ePHI

BAA: acuerdo legal obligatorio que define salvaguardas y responsabilidades

Ejemplos: facturación, transcripción médica, IT, mejora de calidad

■ Redbridge.

Evaluación escrita de vulnerabilidades (confidencialidad, integridad, disponibilidad)

Plan de gestión para mitigar riesgos

Mecanismo clave de cumplimiento y costo-efectivo

■ Redbridge.

Usuarios únicos y contraseñas robustas

Acceso por rol (mínimo necesario)

Registro/auditoría de accesos (logs)

Cierre automático de sesión y cifrado

Derechos del paciente bajo HIPAA

■ Redbridge.

- Acceder a sus registros médicos.
- Solicitar correcciones.
- Recibir un aviso sobre las prácticas de privacidad.
- Solicitar restricciones sobre ciertas divulgaciones de información.

Escenario 1: Filmación sin consentimiento

■ Redbridge.

Campaña promocional quiere grabar consultas

Entrenamiento HIPAA ≠ permiso del paciente

Se requiere consentimiento escrito y posibilidad de retirarlo

Paso recomendado: consultar al Oficial de Privacidad de Redbridge
(Dr Carlos Fernandez email: cfernandez@redbridge.cc)

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

43_PCABP-00077

Escenario 2: Acceso no autorizado en ePHI

 Redbridge.

Acceso a la información de salud protegida.

Personal sin función clínica accede a registros

Violación del principio “need to know”

Requiere controles IT y políticas por rol

Acción correcta: reportar al Oficial de Privacidad

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

43_PCABP-00077

Escenario 3: Solicitud de un periodista

■ Redbridge.

El medio busca entrevistas y testimonios

No divulgar PHI a prensa sin autorización escrita

Acción: declinar y notificar al Oficial de Privacidad

Alternativa: remitir al Oficial de Medios/PR designado

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

43_PCABP-00077

Escenario 4: Divulgación impermisible y ausencia de BAA

■ Redbridge.

Proveedor EHR publica un “reporte de ejemplo” con datos reales

Exposición de nombre, DOB, MRN, diagnósticos

Acción recomendada: reportar a OCR; también consultar al Oficial de Privacidad (Dr Carlos Fernandez email: cfernandez@redbridge.cc)

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

Escenario 5: No revocar accesos tras terminación

 Redbridge.

Ex-empleado accede a registros sin autorización

Riesgo de venta/uso indebido de información

Consecuencias: sanciones civiles y criminales

Lección: desactivar accesos inmediatamente

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

43_PCABP-00077

Escenario 6: Laptop perdida en investigación

 Redbridge.

Dispositivo con datos de investigación/pacientes extraviado

Sin cifrado: alto riesgo de brecha

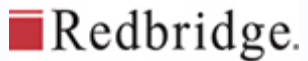
Acción inmediata: informar a supervisor y Oficial de Privacidad

Reforzar políticas de transporte y resguardo de equipos

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

43_PCABP-00077

Escenario 7: Acceder por curiosidad (celebridad)



Acceso sin “need to know” es violación

Conversación informal también puede ser divulgación

Consecuencias: disciplina, despido, reporte al Board

Entrenamiento continuo es esencial

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

Escenario 8: Redes sociales

■ Redbridge.

Publicar detalles clínicos aunque no haya nombre puede identificar

Fotos o historias de pacientes están prohibidas

Acción inicial: documentar (captura/impresión) y llevar al Oficial de Privacidad

Nunca usar redes para comunicar PHI/ePHI

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

43_PCABP-00077

Escenario 9: Citación (subpoena) dudosa

■ Redbridge.

No toda citación obliga a divulgar PHI sin autorización

Verificar autenticidad (membrete, número de caso, firma)

Acción correcta: consultar al Departamento Legal

Cumplir solo según requisitos HIPAA aplicables

Idea clave: aplica el “mínimo necesario” y reporta por el canal oficial.

43_PCABP-00077

Consecuencias de una violación HIPAA

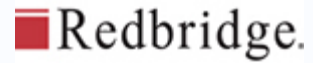
■ Redbridge.

Multas y sanciones (OCR)

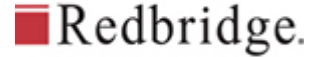
Planes correctivos y monitoreo

Acciones laborales (disciplina/terminación)

Sanciones profesionales y, en casos graves, penales



- Hablar sobre información del paciente en áreas públicas → Utilizar espacios privados.
- Dejar expedientes o pantallas visibles → Bloquear la pantalla y cubrir la información.
- Usar dispositivos personales sin medidas de seguridad → Seguir las políticas de TI.



Los proveedores de atención médica deben cumplir con la **Regla de Notificación de Violaciones de HIPAA**.

Si la información de salud protegida (PHI) se accede, utiliza o comparte de manera indebida, comprometiendo su privacidad o seguridad, deben notificar de inmediato a:

- El Oficial de Privacidad de Redbridge al cfernandez@redbridge.cc

■ Redbridge.

- Acceder a la PHI solo cuando sea necesario para su función.
- Compartir la PHI únicamente con personas autorizadas
- Utilizar canales de comunicación seguros (correo electrónico cifrado, portales seguros).
- Cerrar sesión en los dispositivos cuando no estén en uso o queden desatendidos.
- Reportar inmediatamente cualquier posible o sospecha de violación de seguridad.

HIPAA protege al paciente y refuerza la confianza

El cumplimiento depende de sistemas y conducta diaria

Ante duda: detener, verificar y escalar a Privacidad/Legal

Preguntas

1. Un Case Manager necesita revisar el expediente médico completo de un asegurado para evaluar una preautorización.

¿Cuál es el principio de HIPAA que debe aplicar al acceder a la información?

- a) Acceso irrestricto
- b) Mínimo necesario
- c) Transparencia financiera
- d) Acceso ejecutivo

2. Un proveedor fuera de red solicita enviar registros médicos por correo electrónico sin encriptación.

¿Cuál debe ser la respuesta del equipo de autorizaciones?

- a) Enviar la información inmediatamente
- b) Solicitar un canal seguro y encriptado
- c) Compartir solo datos demográficos
- d) Ignorar la solicitud

3.La aseguradora contrata una empresa externa para auditoría de reclamaciones médicas.

¿Qué requisito es obligatorio antes de compartir PHI?

- a) Firma de acuerdo de confidencialidad simple
- b) Acuerdo de Business Associate (BAA)
- c) Aprobación del proveedor tratante
- d) Autorización del call center

4.Un miembro del equipo comenta en una reunión informal sobre un caso catastrófico identificando país, diagnóstico raro y edad del asegurado.

¿Por qué esto podría ser una violación de HIPAA?

- a) Porque no mencionó el nombre
- b) Porque puede permitir identificación indirecta del paciente
- c) Porque es información financiera
- d) Porque no estaba en horario laboral

5.En el proceso de renovación de póliza, el departamento administrativo revisa información médica previa.

¿Bajo qué categoría se permite esta revisión?

- a) Marketing
- b) Operaciones de salud (PTO)
- c) Acceso público
- d) Investigación académica

References

- Acevedo, N. (2021, October 2). Florida nurse fired after posting photos of baby born with birth defect on social media. *NBC News*. [Visit Source](#).
- Alder, S. (Ed.). (2018, September 13). Texas nurse fired for social media HIPAA violation. *HIPAA Journal*. [Visit Source](#).
- Alder, S. (Ed.). (2023, December 1). What to do if you discover a HIPAA violation in the workplace. *HIPAA Journal*. [Visit Source](#).
- Alder, S. (Ed.). (2019a, March 8). Dozens of Northwestern Memorial Hospital employees fired for accessing Jussie Smollett's medical records. *HIPAA Journal*. [Visit Source](#).
- Alder, S. (Ed.). (2019b, January 3). Summary of 2018 HIPAA fines and settlements. *HIPAA Journal*. [Visit Source](#).
- Alder, S. (Ed.). (2024, January 6). New HIPAA regulations in 2023–2024. *HIPAA Journal*. [Visit Source](#).
- American Recovery and Reinvestment Act of 2009, Pub. L. No. 111–5, § 13001–13424, 123 Stat. 115 (2009).
- Cotter, S. P. (2018, September 21). *ABC News documentary leads to HIPAA violation fines against Boston hospitals*. Boston Herald. Updated November 8, 2019. [Visit Source](#).
- Donovan, F. (2018, June 11). *New York suspends nurse for HIPAA violation affecting 3K patients*. Intelligent Healthcare Media. [Visit Source](#).

6. Un ex empleado mantiene acceso activo al sistema ROS y puede visualizar casos abiertos.

¿Qué salvaguarda de HIPAA falló?

- a) Control físico
- b) Análisis de riesgo
- c) Revocación de acceso tras terminación
- d) Capacitación anual

7. Un asegurado solicita resultados médicos a través de redes sociales privadas.

¿Cuál es la respuesta adecuada?

- a) Enviar la información por mensaje directo
- b) Solicitar que utilice un canal seguro autorizado
- c) Enviar solo parcialmente la información
- d) Ignorar la solicitud

8. ¿Cuál es la función principal del Office for Civil Rights (OCR) en relación con una aseguradora médica internacional que opera en EE.UU.?

- a) Negociar contratos médicos
- b) Investigar y sancionar violaciones de HIPAA
- c) Emitir licencias de seguros
- d) Aprobar primas de pólizas

9.¿Por qué es fundamental que el departamento de Case Management realice análisis de riesgo periódicos en sus sistemas electrónicos?

- a) Para reducir costos operativos
- b) Para cumplir requisitos contractuales únicamente
- c) Para identificar vulnerabilidades y prevenir brechas de ePHI
- d) Para aumentar el volumen de casos

10.En el contexto de evacuaciones médicas internacionales, **¿qué debe verificarse antes de compartir información clínica con un hospital receptor en otro país?**

- a) Que el hospital tenga buenas referencias
- b) Que exista base legal y canal seguro para transferencia de PHI
- c) Que el paciente viaje el mismo día
- d) Que el hospital confirme disponibilidad de cama

- Federal Bureau of Investigation. (2010, January 8). *Ex-UCLA healthcare employee pleads guilty to four counts of illegally peeking at patient records*. Federal Bureau of Investigation. [Visit Source](#).
- Moore, W., & Frye, S. (2020). Review of HIPAA, Part 2: Limitations, rights, violations, and role for the imaging technologist. *Journal of Nuclear Medicine Technology*, 48(1), 17–23. [Visit Source](#).
- Morgan, S. (2018, August 29). *Texas Children’s Hospital nurse fired after social media post*. Fox 26 Houston. [Visit Source](#).
- Quraishi, A. (2019, March 8). *At least 50 Northwestern Hospital employees fired for accessing Smollett’s profile, records: sources*. NBC Chicago. [Visit Source](#).
- Tariq, R. A., & Hackert, P. B. (2023). Patient confidentiality. In *StatPearls*. StatPearls Publishing. [Visit Source](#).
- U.S. Department of Education. (2012). Family Educational Right and Privacy Act regulations (FERPA). Federal Registry, 34, Subparts S and B. Codified at 34 CFR §§ 99.1 – 99.8.
- U.S. Department of Health and Human Services. (2005). *4 Security standards: Technical safeguards*. [Visit Source](#).
- U.S. Department of Health and Human Services. (2010). Public welfare: General provisions and procedures for hearings. Federal Registry, 2, Subparts A and E. Codified at 45 CFR §160.
- U.S. Department of Health and Human Services. (2016, March 17). *Improper disclosure of research participants’ protected health information results in \$3.9 million HIPAA settlement*. [Visit Source](#).