ALTO EL COSTO DEL RIESGO CIBERNÉTICO Y LA NEGLIGENCIA CON HIPAA

En 2025 la Oficina de Derechos Civiles (OCR) del Departamento de Servicios Humanos y de Salud de los EU (DHHS) impuso multas de $25,000 a $3 millones tras la investigación de incidentes de seguridad en los que se identificó negligencia en el cumplimiento con la Ley HIPAA. A la multa ($) se suman miles en costos asociados el manejo del incidente, la investigación, y el ejecutar planes correctivos.

En 2026 urge atender la diligencia en el cumplimiento con HIPAA cuando se accede, crea, mantiene o transmite electrónicamente información protegida de salud (ePHI), ya que:

- ✓ ***La amenaza continua de ataques cibernéticos aumenta el riesgo de incidentes de seguridad.***
- ✓ ***La inteligencia artificial (IA) puede comprometer la privacidad y seguridad de ePHI.***
- ✓ ***El DHHS OCR como fiscalizador continuará aplicando sanciones por violar las Reglas de HIPAA.***

¿Por qué Smart Compliance SC365® es su socio idóneo?

Somos expertos en diligenciar el cumplimiento y reducir el riesgo cibernético para evitar sanciones. Por más de 25 años hemos logrado para nuestros clientes resultados excepcionales con la asertiva integración de servicios especializados con soluciones de vanguardia que potencian una transformación digital centrada en el cumplimiento con HIPAA, NIST, ISO y RGPD. *Certificaciones: HIPAA CHP/CHA, Ciberseguridad CCSA/CMMC, y como Contratista Federal (SAM) SBA: WOSB, EDWOSB, HUBZONE, y 8(A)*.

Hablemos de como potenciamos su entorno digital; contáctanos.

¿Cuándo DHHS OCR impondrá las sanciones por violación a HIPAA?

La sanción podrá ser impuesta cuando la entidad no pueda demostrar su cumplimiento con las Reglas de Privacidad y Seguridad de HIPAA. La Ley HIPAA requiere que la entidad mantenga por 6 años sus políticas, procedimientos, análisis de riesgo, acuerdos, incidentes, y toda documentación para demostrar su diligencia en el cumplimiento ante las investigaciones del Secretario de DHHS OCR.

Smart Compliance SC365® fomentamos su cumplimiento para evitar sanciones; contáctanos.

¿Cuándo un ataque cibernético es un incidente de seguridad?

Un ataque cibernético es un incidente de seguridad cuando el actor o "Hackers" logra infiltrarse a un Activo de Informática y Tecnología (IT); local o remoto, como "Clloud o IoT". También, el incidente puede ocurrir de un acto interno, como empleados o contratistas. El incidente de seguridad es impredecible, pero es prevenible al implementar las salvaguardas de HIPAA: administrativas, técnicas y físicas.

Smart Compliance SC365® fortalecemos su ciberseguridad para reducir los incidentes; contáctanos.

¿Cuándo debe gestionar la notificación de un incidente de seguridad?

La notificación de un incidente de seguridad se hará cuando se identifica una brecha del ePHI, ya sea por un acceso no autorizado, la divulgación indebida, y/o alteración. HIPAA establece directrices sobre a quienes, cómo y cuándo se harán las notificaciones, incluyendo notificar al DHHS OCR. La agencia investiga los incidentes reportados, inclusive en medios noticiosos o redes, y por pacientes o familiares.

Smart Compliance SC365® facilitamos su gobernanza digital para mitigar riesgos; contáctanos.

Presentamos un resumen de los casos publicados por DHHS OCR con sanciones aplicadas a todo tipo de entidad, inclusive socios de negocio, a consecuencia de investigaciones de incidentes y quejas reportados desde el 2018.

Smart Compliance SC365® protegemos su presente y futuro; contáctanos.

OCR Resolution Penalty Date	OCR Resolution HIPAA Penalty ($)	Entity Type	Security Incident Type (Amounts = Individuals/Patient)
18-Aug-2025	$ 175,000.00	Business Associate - CPA	Ransomware - PHI Breach 170,000
23-Jul-2025	$ 250,000.00	Provider – Surgery Center	Unauthorized Access - ePHI Breach 24,981
01-Jul-2025	$ 950,000.00	Provider – Primary Care Clinics	Media Reported Security Incident
30-May-2025	$ 75,000.00	Business Associate - IT Network Services	Unauthorized Access - ePHI Breach 585,621
28-May-2025	$ 800,000.00	Provider - Hospital	Unauthorized Use & Access - One Patient Claim
15-May-2025	$ 25,000.00	Provider - Radiology	Wrongful Online Disclosure - One Patient Claim
25-Apr-2025	$ 25,000.00	Provider - Neurology	Ransomware - ePHI Breach 6,800
23-Apr-2025	$ 600,000.00	Provider – Primary Care Clinics	Phishing Email - ePHI Breach 189,763
17-Apr-2025	$ 25,000.00	Provider - Hospital	Ransomware - ePHI Breach 5,000
04-Apr-2025	$ 350,000.00	Provider - Radiology	Unauthorized Access Internal Staff
21-Mar-2025	$ 227,816.00	Provider – Wellness Consultant	Wrongful Online Disclosure
20-Feb-2025	$ 1,500,000.00	Business Associate - Vision/Eyewear	Hacked Credentials - ePHI Breach 197,986
14-Jan-2025	$ 3,000,000.00	Provider – Medical Supply	Phishing Email - ePHI Breach 114,007
08-Jan-2025	$ 337,750.00	Provider - Behavioral	Unauthorized Access of Business Associate Staff
07-Jan-2025	$ 90,000.00	Business Associate - IT Network Services	Ransomware - ePHI Breach
07-Jan-2025	$ 80,000.00	Business Associate - EHR Software Vendor	Hacked Unauthorized Access - ePHI Breach 31,248
10-Dec-2024	$ 250,000.00	Clearinghouse	Wrongful Online Disclosure - ePHI 1,565,338
01-Dec-2024	$ 1,190,000.00	Provider – Pain Management	Internal Unauthorized Access - 34,310

References:

- ***Summary of the HIPAA Security Rule | HHS.gov***
- ***Resolution Agreements | HHS.gov***
- ***Smart Compliance SC365® HIPAA Compliance & Cybersecurity Framework***