

## **Violaciones comunes de HIPAA que se deben evitar**

A continuación, se detallan algunas de las violaciones más comunes de HIPAA y cómo evitarlas:

1. Consultar registros médicos sin permiso ni autorización:  
Asegúrese de que el acceso a los registros médicos de los pacientes sólo sea para fines de tratamiento, pago u operaciones de atención médica.
2. No realizar un análisis de riesgos a nivel de toda la organización:  
Realice evaluaciones de riesgo de HIPAA periódicas para detectar dónde la PHI es vulnerable.
3. No abordar los riesgos de seguridad:  
Priorizar la atención de cualquier riesgo que se identifique durante las auditorías.
4. Negar a los pacientes el acceso a sus historiales médicos:  
Proporcionar a las personas acceso a sus registros médicos cuando lo soliciten y sin demora.
5. Incumplimiento de un Acuerdo de Asociado Comercial que cumpla con la HIPAA:  
Asegúrese de que todos los proveedores externos con acceso a PHI también mantengan el cumplimiento de HIPAA.
6. Medidas de control de acceso a ePHI insuficientes:  
Asegúrese de que las personas autorizadas sean las únicas que puedan acceder a la información médica electrónica protegida (ePHI).
7. No utilizar cifrado o seguridad equivalente para salvaguardar la ePHI:  
El cifrado no es obligatorio según HIPAA, pero medidas de seguridad iguales deben proteger la ePHI.
8. Superar el plazo de 60 días para las notificaciones de infracciones:  
Si su organización descubre una violación de datos, debe notificar a las personas afectadas por escrito dentro de los 60 días.
9. Divulgaciones de PHI no autorizadas:  
Los pacientes deben autorizar cualquier intercambio de su PHI.
10. Eliminación inadecuada de PHI:  
Debe destruir de forma segura y permanente la PHI cuando ya no sea necesaria.
11. Descargar PHI en dispositivos no autorizados:  
Los empleados solo deben utilizar dispositivos autorizados que estén conectados a la red y sean seguros para acceder a la PHI.
12. Envío de ePHI a una cuenta de correo electrónico personal:  
Asegúrese de que los empleados no envíen ePHI a sus cuentas de correo electrónico personales ni eliminen de otro modo ePHI del centro de atención médica.

<https://secureframe.com/es-es/hub/hipaa/violations>