NATIONAL CONSORTIUM OF TELEHEALTH RESOURCE CENTERS

La HIPAA y la telesalud

Una guía paso a paso para cumplirlas

¿Debería preocuparme?

PASO 1

¿SE APLICA LA HIPAA A MÍ Y A MIS SERVICIOS DE TELESALUD?
La HIPAA se aplica a usted si es un proveedor de atención médica que envía información médica personal (PHI) de forma electrónica. Si es así, usted ES una entidad cubierta (CE).

PASO 2

¿SE CONSIDERA LA INFORMACIÓN QUE ESTOY TRANSMITIENDO COMO PHI? Cualquier cosa que se pueda usar para identificar a una persona es muy probable que sea PHI. Hay 18 tipos de identificadores que se consideran PHI. Los ejemplos relacionados con la telesalud incluyen: nombres, teléfonos, fechas de nacimiento, direcciones de IP, direcciones de correo electrónico, identificadores de dispositivos y fotografías o imágenes.

PASO 3

¿TENGO SOCIOS COMERCIALES? Un socio comercial es cualquier socio que cree, reciba, conserve o transmita PHI en su nombre, o tenga la capacidad de tener contacto con la PHI en su consultorio médico. Consulte los ejemplos de PHI arriba.

BIEN. ¡YA ME PREOCUPÉ! **Siga leyendo para saber qué puede hacer.**

¿Sabía que...?

1. Si comparte cualquier tipo de información con socios comerciales, cualquier error que ellos cometan al proteger la seguridad y privacidad de su información es también su error. USTED sigue siendo responsable.
2. Que usted cumpla la ley ahora depende de las prácticas de sus socios.
3. Puede protegerse firmando acuerdos de socios comerciales (BAA) que obliguen a documentar cómo protege el socio su PHI e implementando procesos razonables para verificar las prácticas de seguridad de los socios.

No le revele PHI a ningún socio comercial que no quiera firmar un BAA.

Cómo cumplir con la HIPAA

Para cumplir con la HIPAA hay que combinar medidas de protección físicas, administrativas y técnicas. La tecnología por sí misma no puede cumplir con la HIPAA ni hacer que usted la cumpla. Esto es lo que usted y sus socios comerciales deberían hacer y documentar:

EVALUACIÓN DEL RIESGO: revisar cuidadosamente en dónde guardan o tienen acceso a la PHI y qué tan seguro es en cada caso. Seguir los pasos adecuados para asegurarla de una forma que se ajuste a su organización. Establecer y documentar sus políticas y procedimientos de seguridad. Capacitar a sus empleados con regularidad y constancia.

REVISIÓN DE LA ACTIVIDAD DE LOS SISTEMAS DE INFORMACIÓN: hacer y documentar revisiones periódicas de los registros de acceso y otros registros en busca de actividad no autorizada. Podrían ser malas noticias si encuentra algo, pero querrá ser USTED el primero en descubrirlo. Informar de la vulneración y solucionarla de inmediato. Hable con su asesor jurídico sobre qué pasos seguir.

También es recomendable que considere formas de configurar su sistema para que la PHI no se guarde ni se comparta.

Cuatro preguntas que debería hacerle a su posible socio comercial

...aunque todos digan que cumplen con la HIPAA.

Pregunta 1:
¿A cuál de los 18 identificadores de PHI PODRÍA su empresa tener acceso?

Pregunta 2:
¿Puedo ver los resultados de su última auditoría de cumplimiento de la HIPAA?

Pregunta 3:
¿Qué medidas de protección administrativas, físicas y técnicas tiene vigentes?

Pregunta 4:
¿Estaría dispuesto a firmar NUESTRO BAA?

Créditos extra

¡Compare estas mediciones entre proveedores!

Recordatorio...

La encriptación por sí misma no es cumplir con la ley, y los procesos que cumplen con la ley en una relación entre clínicas podrían no cumplirla en una relación entre la clínica y el consumidor. El contexto es importante.

Cosas que debe recordar CUANDO (no SI) tiene una vulneración...

¿Qué está en juego?

INFRACCIONES NO INTENCIONADAS
«Pero yo no sabía»

$100 mínimo por infracción

$50,000 máximo por infracción

MANTENGA LA CALMA
Si corrige la primera infracción en un plazo de 30 días, podría evitar las sanciones.

Sanciones económicas

INFRACCIONES NEGLIGENTES INTENCIONADAS
«Pero usted sí sabía*»

Corregida en el tiempo requerido — $10,000+ por infracción

No corregida — $50,000+ por infracción

*Solo es necesario saber sobre las acciones que constituyen una infracción. No es necesario saber específicamente que una acción particular viola la ley HIPAA.

Multas + sanciones penales + civiles

La sanción máxima es de $1.5 millones al año por infracción

Obtenga más información sobre la HIPAA

- *Oficina de Derechos Civiles de los HHS
- *Centro de Políticas sobre Salud Conectada
- *Código Electrónico de Reglamentos Federales
- *HIPAA.com
- *Aclaraciones del UMTRC sobre la HIPAA
- *Kit de herramientas de NIST para las normas de seguridad de la HIPAA
- *La Asociación Médica Americana y la HIPAA

¿Tiene preguntas? Comuníquese con un Centro de Recursos de Telesalud