safetica

Cómo ayuda Safetica a cumplir con la HIPAA

Versión: 2022-08-0

Introducción a HIPAA

La Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus siglas en inglés) se diseñó inicialmente para mejorar la portabilidad de la cobertura de seguro médico para las personas que estaban en transición de empleos. Antes de esta ley, los empleados corrían el riesgo de perder su cobertura médica durante los periodos de transición laboral.

Otro objetivo fundamental de la HIPAA era asegurar la adecuada protección de todos los datos relacionados con la salud, garantizando que ningún individuo no autorizado pudiera acceder a dicha información sensible.

La aplicación de la HIPAA se extiende a las organizaciones en los Estados Unidos y está sujeta a regulación por parte de la Oficina de Derechos Civiles (OCR) del Departamento de Salud y Servicios Humanos.

Propósito de HIPAA

La HIPAA fue creada con el objetivo de modernizar el flujo de información en el ámbito médico y garantizar la protección de Identificación Personal recopilada en empresas de salud y seguros, evitando fraudes, robos y asegurando que no pueda divulgarse sin el consentimiento correspondiente.

La información de salud de los pacientes se trata con mayor sensibilidad y puede ser accedida rápidamente por diversos proveedores de atención médica. Las regulaciones de la HIPAA requieren que los registros estén más seguros y protegidos contra posibles filtraciones.

¿Qué es la Información Médica Protegida (PHI)?

La PHI se crea cuando cualquier dato de salud se combina con información de identificación personal, como nombre, correo electrónico, números de cuenta, número de registro médico, fotografías de rostro completo, números de Seguro Social, etc. Cuando la PHI se almacena electrónicamente, se denomina ePHI.

El alcance de la HIPAA

Hay varias entidades que trabajan regularmente con información médica protegida y, por lo tanto, deben cumplir con la Ley de Portabilidad y Responsabilidad de Seguros Médicos:

- Proveedores de atención médica
- Planes de salud
- Centros de intercambio de información sobre el sector salud

- Socios comerciales

Desafíos relacionados y cómo Safetica ayuda a superarlos

1. Mantener la privacidad y confidencialidad de la PHI

La Ley de Privacidad requiere que se asegure los registros de pacientes que contienen PHI, para que no estén fácilmente disponibles para aquellos que no necesitan verlos.

Al utilizar la inspección de contenido con OCR, Safetica puede clasificar automáticamente los datos de PHI y aplicar políticas de DLP que definen dónde se pueden almacenar dichos datos, dónde se permite que fluyan y cómo. Esto garantiza que se aplique el almacenamiento seguro y que el acceso a la PHI se pueda limitar solo al personal crítico.

Dependiendo como esté configurada la solución de Safetica, puede bloquear la actividad de riesgo, notificar al usuario (y al administrador), redirigir a los empleados a las pautas de seguridad de la organización o permitirles justificar la operación restringida.

2. Compartir información con otros profesionales de la salud

La Ley de Privacidad requiere que usted proteja los registros de pacientes que contienen PHI cuando se comparten con otros Profesionales de la Salud.

Safetica facilita la gestión y el control de dónde se pueden almacenar los datos sensibles y los destinos (canales de datos) desde los que pueden salir los datos de un departamento u organización. El flujo de datos de PHI que Safetica detecta y clasifica automáticamente se puede controlar mediante políticas DLP simples.

Las directivas DLP pueden impedir que la PHI abandone una organización. Además, se puede definir un perímetro (zona) seguro para especificar los destinatarios autorizados y los terceros que pueden trabajar con los datos sin restricciones. Todo esto está sujeto a un monitoreo continuo; todas las acciones, bloqueadas o permitidas, se registran para auditorías y fines de investigación.

Una característica opcional permite a usuarios específicos anular una política de seguridad existente. Con este modo DLP, un usuario debe proporcionar una justificación comercial, que luego se registra y se informa al personal de seguridad. Esto permite a los usuarios seleccionados anular políticas de seguridad restrictivas en caso de necesidad urgente, pero también comunica al personal de seguridad lo que se requería y por qué.

3. Compartir información con los miembros de la familia

La Ley de privacidad le permite comunicarse con familiares identificados y aprobados, siempre y cuando utilice medidas de seguridad para proteger la privacidad y confidencialidad de la PHI de los pacientes.

La solución de Safetica ofrece una opción para incluir en la lista blanca de destinatarios autorizados, igualmente monitoreados, para recibir PHI y otros datos confidenciales.

4. Notificaciones de incumplimiento

Cuando experimenta una violación de PHI, la Ley de notificación de incumplimiento HIPAA requiere que notifique a las personas afectadas, al HHS y, en algunos casos, a los medios de comunicación.

En caso de un incidente o un intento de fuga de datos , el sistema de alerta por correo electrónico en tiempo real de Safetica notifica al personal correspondiente. Informa rápidamente del incidente y proporciona suficientes detalles para que puedan evaluar el impacto de la situación y tomar medidas de seguimiento.

Safetica también proporciona amplios registros de auditoría sobre operaciones realizadas con datos confidenciales. Esto ayuda a identificar la profundidad de la infracción, los documentos confidenciales afectados y las personas afectadas.

Con la integración de API, todos los registros también se pueden enviar a SIEM o herramientas de análisis de datos, por ejemplo, Power BI o Tableau.

5. Cifrado de datos de PHI almacenados en dispositivos de endpoint

La HIPAA requiere varias medidas de seguridad para proteger la PHI cuando se almacenan datos. Uno de estos requisitos es el cifrado.

Safetica ayuda a las organizaciones a administrar el cifrado de almacenamiento (Microsoft BitLocker), protegiendo así los datos en reposo. El cifrado se gestiona de forma centralizada en la consola de gestión de Safetica, con claves de cifrado distribuidas de forma segura entre dispositivos de punto final seguros, lo que elimina la necesidad de compartirlas entre usuarios.

Caso de uso clave

Proveedor de software para el sector salud

Un proveedor líder en EE. UU. de aplicaciones de gestión de consultorios y software de automatización y facturación médica para organizaciones de atención médica necesita proteger los datos de los pacientes y cumplir con HIPAA.

Problema: La empresa procesa una gran cantidad de datos que pueden aparecer en cualquier parte del entorno. Por lo tanto, necesitan saber dónde están los datos, quién trabajó con ellos y cómo. Un sistema de tickets para este software de facturación médica también puede procesar capturas de pantalla y otras solicitudes de los clientes que podrían contener datos de pacientes que requieren una protección adecuada.

Solución: La combinación de Safetica ONE Enterprise con el módulo UEBA proporciona un descubrimiento y clasificación de datos unificados y flexibles. Las políticas de contenido que utilizan plantillas integradas para PII e HIPAA le darán al cliente una visión general de dónde están los datos confidenciales y hacia dónde fluyen.

La configuración de varias zonas seguras ayudará a definir áreas específicas en las que es seguro trabajar con datos sin restricciones estrictas. El control de dispositivos solo permite a los usuarios conectar dispositivos USB aprobados por la empresa a sus computadoras. Todos los datos deben estar encriptados y el cifrado de Bitlocker se puede administrar desde la consola central de Safetica.

Safetica puede clasificar todas las descargas desde el servidor del sistema de emisión de tickets y solo permitir las cargas de vuelta al sistema o a la unidad de red protegida.

Resultados: La empresa cumple continuamente con los requisitos de cumplimiento de HIPAA. Con Safetica, la empresa entiende dónde pueden aparecer los datos confidenciales y puede controlar cómo se permite que los datos se muevan dentro de sus sistemas. Safetica ONE Enterprise también ofrece opciones de integración con Microsoft 365 y Microsoft Information Protection. Las notificaciones de seguridad de datos de Safetica ONE se envían a SIEM para su posterior análisis. El resto de los registros se guardan en la consola de administración de Safetica.

Excelente protección de datos simplificada

safetica

www.safetica.com