Seguridad de los datos para agentes de UnitedHealthcare

Descripción general del programa y Preguntas Frecuentes (Frequently Asked Questions, FAQ)

United Healthcare

Descripción general del programa

En UnitedHealthcare, proteger la seguridad y la privacidad de los datos es nuestra prioridad. A medida que evolucionan los riesgos cibernéticos y de privacidad, nos mantenemos firmes en nuestro compromiso de proteger la información de nuestros miembros y afiliados.

Como agente de UnitedHealthcare, debes participar en el proceso de revisión y verificación de la seguridad de los datos. Como miembro valioso de nuestro equipo de distribución, nos gustaría colaborar contigo para garantizar que tus controles de seguridad de los datos y procesos de cifrado sean robustos, reduzcan al mínimo posible los riesgos y brinden servicios de forma eficaz a nuestros clientes mutuos.

Juntos, podemos mantener los más altos estándares de seguridad y privacidad de los datos.

1. **¿Qué actividades de seguridad deben realizar los corredores?**

   El programa de seguridad de UnitedHealthcare se aplica a todos los corredores y agencias de UHC. Incluye:

   - Certificaciones o cuestionarios de seguridad en línea
   - Revisiones periódicas de seguridad
   - Corrección de los hallazgos de seguridad correspondientes

   Estas actividades evalúan la infraestructura de seguridad para garantizar que se implementen los controles administrativos, técnicos y físicos adecuados. Esto se realiza para proteger la información del cliente, como se describe en el contrato de UnitedHealthcare y los requisitos para asociados comerciales de la Ley de Portabilidad y Responsabilidad del Seguro Médico (Health Insurance Portability and Accountability Act, HIPAA).

2. **¿Cuál es el objetivo de una certificación y un cuestionario?**

   El proceso comienza con una certificación o cuestionario de seguridad en línea. Estas medidas están diseñadas para autoinformar el cumplimiento de los requisitos de control de privacidad y seguridad, y garantizar que los corredores cumplan con los estándares establecidos por la HIPAA y los contratos de UnitedHealthcare. Las certificaciones y los cuestionarios se envían de forma periódica a lo largo del año.

3. **¿Qué es una revisión de seguridad?**

   El siguiente paso del proceso es una revisión de seguridad. Esta revisión es facilitada por un analista de seguridad de UHC designado, quien se pondrá en contacto contigo para programar una reunión virtual a través de Microsoft Teams. Durante la reunión, el agente mostrará los controles de seguridad correspondientes al compartir la pantalla o proporcionando capturas de pantalla.

4. **¿Qué controles de seguridad se revisarán?**
   Dependiendo del entorno empresarial, se revisan hasta 8 controles de seguridad clave. El analista de seguridad de UHC asignado proporciona la información de control correspondiente antes de la reunión. Consulta “Controles para la revisión de la seguridad” más adelante para obtener más detalles.

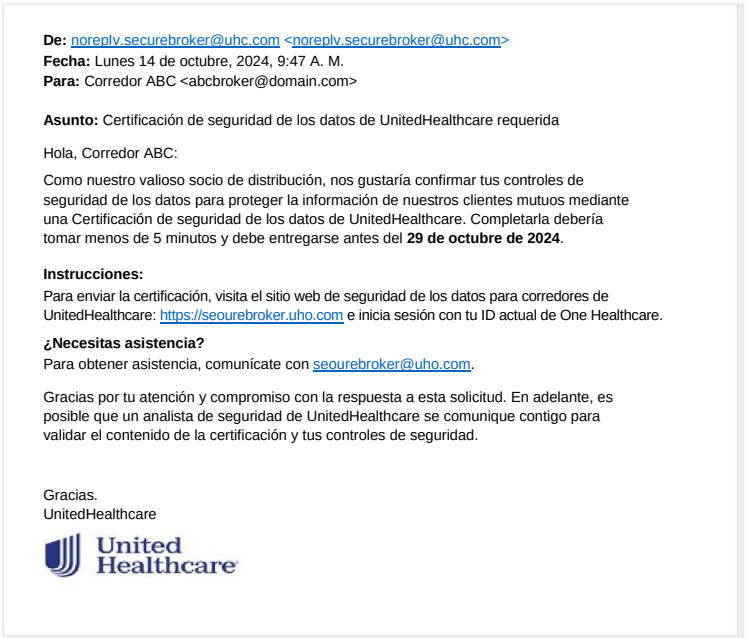
5. **¿Qué sucede si los controles *no* están implementados para la revisión de la seguridad?**
   Si los controles no están implementados antes o después de la revisión de la seguridad, el analista de UHC explicará los requisitos y proporcionará indicaciones estándar de la industria. Un analista de UHC realizará un seguimiento periódico con la agencia hasta que se implementen los controles restantes y se demuestren las pruebas.

6. **¿Con quién debo comunicarme si tengo preguntas?**
   Comunícate con securebroker@uhc.com y un analista de seguridad de UHC te ayudará.

7. **¿Cuándo se comunicará a las agencias?**
   UnitedHealthcare se comunicará de forma periódica con los agentes por correo electrónico para brindarles instrucciones e indicaciones sobre las actividades requeridas. Este es un proceso continuo y se comunicará a los agentes a lo largo del año.
   Direcciones web y de correo electrónico utilizadas:

   - Correo electrónico inicial: noreplv.securebroker@uhc.com

     Correo electrónico de ejemplo:



De: noreplv.securebroker@uhc.com <noreplv.securebroker@uhc.com>
Fecha: Lunes 14 de octubre, 2024, 9:47 A. M.
Para: Corredor ABC <abcbroker@domain.com>

Asunto: Certificación de seguridad de los datos de UnitedHealthcare requerida

Hola, Corredor ABC:

Como nuestro valioso socio de distribución, nos gustaría confirmar tus controles de seguridad de los datos para proteger la información de nuestros clientes mutuos mediante una Certificación de seguridad de los datos de UnitedHealthcare. Completarla debería tomar menos de 5 minutos y debe entregarse antes del **29 de octubre de 2024**.

Instrucciones:
Para enviar la certificación, visita el sitio web de seguridad de los datos para corredores de UnitedHealthcare: https://seourebroker.uho.com e inicia sesión con tu ID actual de One Healthcare.

¿Necesitas asistencia?
Para obtener asistencia, comunícate con seourebroker@uho.com.

Gracias por tu atención y compromiso con la respuesta a esta solicitud. En adelante, es posible que un analista de seguridad de UnitedHealthcare se comunique contigo para validar el contenido de la certificación y tus controles de seguridad.

Gracias.
UnitedHealthcare

- Portal de seguridad: https://securebroker.uhc.com

Controles de revisión de la seguridad

Esta sección ofrece una descripción general y describe las pruebas de validación necesarias para una revisión de la seguridad. El analista de seguridad de UHC colaborará con los agentes para identificar los controles correspondientes a tu entorno empresarial y técnico específico.

1. Autenticación Multifactor (Multi Factor Authentication, MFA): Los empleados remotos o los terceros que acceden a los sistemas del agente utilizan la autenticación multifactor para evitar el acceso no autorizado a su red interna.

Captura de pantalla del mensaje de inicio de sesión secundario de MFA cuando un empleado inicia sesión de forma remota

2. Identificación y autenticación del usuario: Gestión del acceso de los empleados a aplicaciones, estaciones de trabajo, instalaciones y redes.

Documento de políticas y procedimientos que abarca lo siguiente:
a) A cada empleado se le asigna su propia ID de usuario única
b) Configuración de contraseñas estándar de la industria
c) Proceso para agregar y eliminar el acceso de los empleados a computadoras, aplicaciones e instalaciones

3. Realización de evaluaciones de riesgo: Se realiza una evaluación de riesgos anual que abarca los riesgos físicos, administrativos y técnicos, de acuerdo con un asociado comercial de la HIPAA. Esta actividad debe documentarse formalmente.

Copia del informe de evaluación de riesgos más reciente, con las modificaciones necesarias

4. Cifrado de disco completo: Se implementa una solución de cifrado en los activos que acceden a la información de los miembros, lo que reduce la posibilidad de acceso o divulgación no autorizados de los datos debido a malware y robo o pérdida de dispositivos.

Captura de pantalla de un ejemplo de estación de trabajo de un empleado (como computadora de escritorio, computadora portátil o dispositivo móvil) con cifrado de disco completo

Si corresponde, una captura de pantalla que valide que los servidores estén cifrados con AES/256 bits

5. Controles de entrada física: Se garantiza que solo las personas autorizadas tengan acceso a las instalaciones, servidores y hardware crítico del agente. Según las guías de la HIPAA, la organización es responsable de determinar las medidas de seguridad física adecuadas.

Documento de políticas y procedimientos que detalla la seguridad física

6. Administración de medios extraíbles: Restringe el uso de medios extraíbles, como USB o discos duros externos, debido a que es fácil que se pierdan datos y se transfiera código malicioso a través de ellos.

Documento de políticas y procedimientos que abarca la administración de medios extraíbles

Captura de pantalla de la configuración establecida para bloquear o restringir el uso de medios extraíbles

7. Análisis de vulnerabilidades y administración de aplicación de revisiones: Se realizan análisis periódicos en redes y puntos de conexión para detectar vulnerabilidades y aplicar revisiones a estas vulnerabilidades. Las vulnerabilidades en la red, los sistemas operativos, los dispositivos de red y los navegadores web de la organización pueden ser explotadas por usuarios maliciosos si no se detectan ni se solucionan.

Copia redactada del análisis de vulnerabilidades de red más reciente y del informe de aplicación de revisiones

Documento de políticas y procedimientos que abarca la gestión de aplicación de revisiones y el análisis de vulnerabilidades

Evidencia de un Sistema Operativo (Operating System, OS) compatible con el fabricante configurado para recibir actualizaciones automáticas

8. Antivirus y antimalware: El antivirus está instalado y configurado en los activos para proteger contra código malicioso, lo cual puede resultar en acceso no autorizado, comprometer la información de los clientes y causar interrupciones en el servicio.

Capturas de pantalla del antivirus configurado para recibir actualizaciones diarias de firmas y analizar el sistema cada 24 horas.

Recursos de privacidad y seguridad

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

https://www.healthit.gov/providers-professionals/security-risk-assessment-tool