UnitedHealthcare Broker Data Security

Program Overview and Frequently Asked Questions (FAQ)

UnitedHealthcare

Program Overview

As a UnitedHealthcare broker or agent, you are required to participate in the annual data security review and verification process. As a valued member of our distribution team, we would like to collaborate with you to ensure that your data security controls and encryption processes are robust, minimizing risk and effectively serving our mutual customers.

Together, we can uphold the highest standards of data security and privacy.

1. **What security activities are brokers and agencies required to complete?**
   UnitedHealthcare's annual security program applies to all UnitedHealthcare brokers and agencies. It includes:

   - Online Security Attestations or Questionnaires
   - Periodic Security Reviews
   - Remediating applicable security findings

   These activities evaluate the security infrastructure to ensure that appropriate administrative, technical, and physical controls are in place. This is done to protect customer information as outlined in the UnitedHealthcare contract and HIPAA Business Associate requirements.

2. **What is the purpose of an Attestation and Questionnaire?**
   The process begins with an on-line security attestation or questionnaire. These measures are designed to self-report compliance with privacy and security control requirements and ensure that brokers and agencies meet the standards set by HIPAA and UnitedHealthcare contracts.

3. **What is a Security Review?**
   The next step of the process is a Security Review. This review is facilitated by a designated UnitedHealthcare Security Analyst who will contact you to set up a Microsoft Teams virtual meeting. During the meeting, the broker or agency demonstrates applicable security controls by screen share or providing screenshots.

4. **What security controls will be reviewed?**
   Depending on the business environment, up to 8 key security controls are reviewed. The assigned UHC Security Analyst provides the applicable control

information in advance of the meeting. Please see 'Security Review Controls' below for additional details.

5. **What happens if the controls are *not* in place for the Security Review?**
   If the controls are not in place prior to or after the Security Review, the UnitedHealthcare Security Analyst will explain the requirements and provide industry-standard guidance. A UnitedHealthcare Security Analyst will follow up periodically with the broker or agency until any remaining controls are in place and evidence is demonstrated.

6. **Who do I contact with questions?**

   Contact securebroker@uhc.com and a UHC Security Analyst will assist.

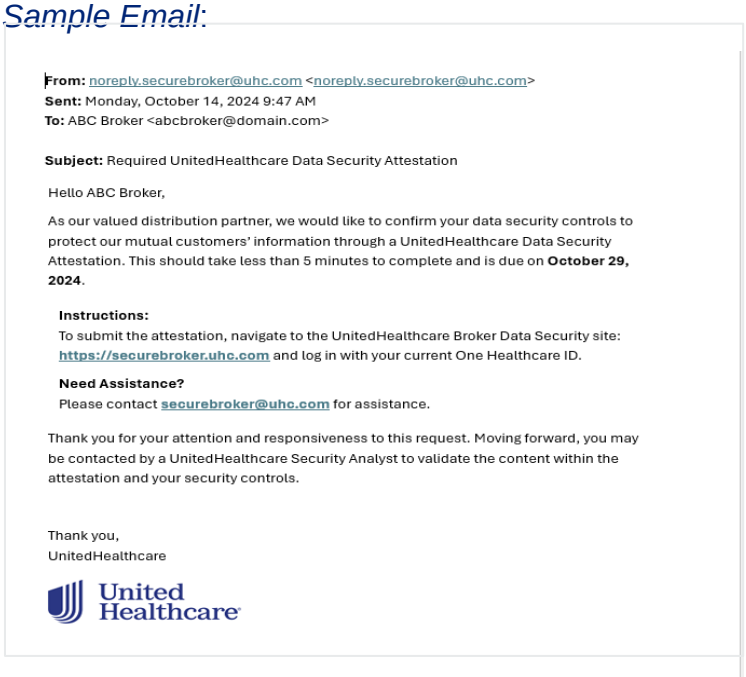
7. **When will brokers and agencies be contacted?**

   UnitedHealthcare will periodically contact brokers and agents via email to provide instructions and guidance on required activities. This is a continuous process, and brokers and agents will be contacted throughout the year.

   Web and email addresses used:

   - Initial email: noreply.securebroker@uhc.com

     Sample Email:



From: noreply.securebroker@uhc.com <noreply.securebroker@uhc.com>
Sent: Monday, October 14, 2024 9:47 AM
To: ABC Broker <abcbroker@domain.com>

Subject: Required UnitedHealthcare Data Security Attestation

Hello ABC Broker,

As our valued distribution partner, we would like to confirm your data security controls to protect our mutual customers' information through a UnitedHealthcare Data Security Attestation. This should take less than 5 minutes to complete and is due on **October 29, 2024**.

Instructions:
To submit the attestation, navigate to the UnitedHealthcare Broker Data Security site: **https://securebroker.uhc.com** and log in with your current One Healthcare ID.

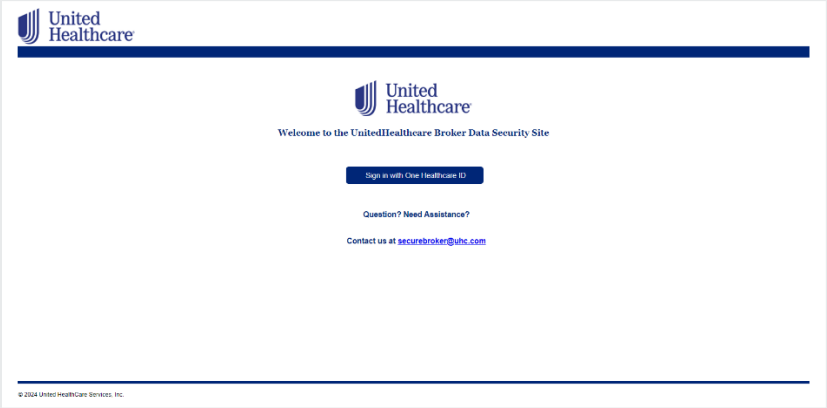
Need Assistance?
Please contact **securebroker@uhc.com** for assistance.

Thank you for your attention and responsiveness to this request. Moving forward, you may be contacted by a UnitedHealthcare Security Analyst to validate the content within the attestation and your security controls.

Thank you,
UnitedHealthcare

United Healthcare

- Security portal: https://securebroker.uhc.com



Security Review Controls

This section provides an overview and outlines the validation evidence required for a Security Review. The UHC Security Analyst will collaborate with brokers and agencies to identify which controls are applicable to their specific business and technical environment.

1. Multi Factor Authentication (MFA): Remote employees or third parties accessing the broker's or agency's systems are using Multi-Factor Authentication to prevent unauthorized access into their internal network.

Screenshot of the secondary MFA login prompt when an employee logs in remotely

2. User Identification and Authentication: Management of employees' access to applications, workstations, facilities, and networks.

Policy and procedure document that covers:
a) Each employee is assigned their own unique user ID
b) Industry-standard password settings
c) Process for adding & removing employee access to computers, applications, and facilities

3. Performing Risk Assessments: An annual risk assessment is performed covering physical, administrative, and technical risks in accordance with a HIPAA Business Associate. This must be a formally documented activity.

Copy of most recent risk assessment report, redacted as necessary

4. Full Disk Encryption: Encryption solution is in place on assets that access member information, reducing the possibility of unauthorized data access or disclosure resulting from malware and lost or stolen devices.

Screenshot of an example employee workstation (such as, desktop, laptop, mobile device) that has full disk encryption

As applicable, a screenshot validating servers are AES/256 bit encrypted

5. Physical Entry Controls: Ensures that only authorized individuals have access to the broker's or agency's facilities, servers, and critical hardware. Per HIPAA guidelines, it's up to the organization to determine what physical security measures are appropriate.

Policy and procedure document that details the physical security

6. Management of Removable Media: Restricts the use of removable media, such as USB or external hard drives, due to the ease of data loss and malicious code that can be transferred via that method.

Policy and procedure document that covers management of removable media

A screenshot of settings in place to block or restrict removable media

7. Vulnerability Scanning & Patch Management: Periodic scans are performed on networks and endpoints for vulnerabilities and patches these vulnerabilities accordingly. Weaknesses in the organization's network, operating systems, network devices, and web browsers may be exploited by malicious users if left undetected and unaddressed.

Redacted copy of the most recent network vulnerability scan and patch report

Policy and procedure document that covers patch management and vulnerability scanning

Evidence of manufacturer-supported Operating System (OS) set to receive automatic updates

8. Anti-Virus & Anti-Malware: Antivirus is in place and configured on assets to protect against malicious code, which may result in unauthorized access, compromise of customer information, and disruption of service.

Screenshots of anti-virus set to receive daily signature updates and scan the system every 24 hours

Privacy and Security Resources

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