UnitedHealthcare Broker Data Security

Program Overview and Frequently Asked Questions (FAQ)

United Healthcare

Program Overview

At UnitedHealthcare, we take data security and privacy seriously. As cyber and privacy risk changes, we are committed to protecting customer and member information. One of your responsibilities in that commitment as a UnitedHealthcare agent requires you to participate in the data security review and verification process. As a member of our valued distribution team, we would like to work with you to confirm that your data security controls and encryption processes minimize risk and effectively operate on behalf of our mutual customers.

I. What security activities are brokers required to complete?

UnitedHealthcare's security program is applicable to all UnitedHealthcare brokers and agencies and includes online security Questionnaires, Attestations, and periodic Security Reviews. The purpose of these activities is to ensure appropriate administrative, technical, and physical controls are in place to protect customer information as outlined in the UnitedHealthcare contract and as a HIPAA Business Associate.

II. What is a Security Review?

The UnitedHealthcare Broker Security Review is an assessment, facilitated by a UnitedHealthcare Security Analyst, using a Microsoft Teams virtual meeting. During the meeting, the broker demonstrates, via screenshare or screenshot, that the applicable security controls are in place.

III. What security controls will be reviewed?

Depending on the business environment, up to 8 key security controls are reviewed. The assigned UnitedHealthcare Security Analyst provides the applicable control information in advance of the meeting. Please see 'Security Review Controls' below for additional details.

IV. 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 Analyst will explain the requirements and provide industry-standard guidance. A UnitedHealthcare Analyst will follow up periodically with the agency until any remaining controls are in place and evidence is demonstrated.

V. Who do I contact with questions?

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

VI. When will agencies be contacted?

UnitedHealthcare will periodically contact agents by email to provide instructions and guidance on what activities need to be completed. This is an ongoing process and agents will be contacted throughout the year.

Web and email addresses used:

- Initial email: noreply.securebroker@uhc.com
- Support mailbox: securebroker@uhc.com
- Security portal: https://securebroker.uhc.com

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

Security Review Controls

This section covers the overview and the validation evidence required in a Security Review. Please note that the UnitedHealthcare Security Analyst will work with brokers to determine which of the controls apply to their specific business and technical environment.

1. Multi Factor Authentication (MFA): Remote employees or third parties accessing the broker'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 facilities, servers, and critical hardware. Per Health Insurance Portability and Accountability Act (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