Sales Policy Job Aid

Privacy and Security

CONTENTS

Overview

UnitedHealthcare, its employees and contractors (such as agents) have an ethical and regulatory obligation to take measures to protect consumer information received against theft and/or misuse.

This obligation stems from the regulatory requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). HIPAA indicates that health insurance carriers as well as their downstream entities (such as plan representatives or agents) must meet its requirements.

Put very simply, HIPAA applies to anyone who provides health care, pays for its coverage, or manages data on behalf of those entities. It requires protection of the information belonging to individuals who are served by those entities.

Your obligation is reinforced by your contract with UnitedHealthcare under the Business Associate Addendum, Exhibit C, in the Agent/Agency Agreement that requires you to implement appropriate administrative, physical, and technical safeguards to protect consumer information.

Protected information includes:

- **Personally Identifiable Information (PII)** associated with the activities conducted by those who the act covers. PII includes any combination of name, date of birth, contact information, identification numbers (including but not limited to SSN, MBI#, bank account or credit card numbers) that can be traced back to an individual.
- **Protected Health Information (PHI)** about health status, activities, or care (past, present or future) associated with individual PII by the entities covered under the act.

HIPAA requirements protect PII/PHI by requiring that its use is limited to those who are duly authorized to view and use their information to carry out activities on their behalf. Duly authorized individuals not only include the previously mentioned entities but also individuals who have been granted authority (such as through a power of attorney or court order) to be a consumer’s legally authorize representative.

Minimally necessary is a rule that must be applied to all your activities with any PII and/or PHI you have been provided or to which you have been granted access. This means that you must limit the information you request or use to the minimum necessary PII/PHI to perform the task you have been authorized to perform. Any information beyond the minimal necessary must not be used or requested.

Agents who fail to protect consumer/member PHI/PII may be subject to financial responsibility for the payment of identity theft protection (e.g., LifeLock) for impacted members resulting from the loss of a device containing PHI/PII (e.g., laptop, mobile/smart phone, or other portable electronic devices) and to corrective and/or disciplinary action up to and including termination.

Protective Measures

Use the safeguards below to help ensure proper handling of PHI/PII and maintenance of consumer privacy.

Governance Procedures

- Annually perform a HIPAA Risk Assessment covering administrative, physical, and technical controls. A free HHS tool is available at: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.
- For your place of business have documented physical entry policies and procedures.

Hardcopy Documents

- Carry only the minimum necessary information to complete the day's activities.
- Conceal documents in a folder or in a locked briefcase when out of the office. Never leave hard copy documents unattended in an area where the documents could be viewed by others (e.g., desk, vehicle, table, or booth). Always keep the folder or briefcase at hand.
- Secure completed lead cards/business reply cards collected during events or in a collection station.
- Secure documents in a locked area when not in use (e.g., file cabinet).
- Dispose of documents containing PHI/PII in a secure manner (e.g., shredded).

Fax

- Verify fax numbers before use to ensure the intended recipient receives the document.
- Use a fax cover sheet that displays a HIPAA Privacy Statement.

Verbal Usage

- Only speak with individuals with express permission or authority to receive the consumer's PII/PHI.
- Avoid and discourage gossip about a consumer's or member's information.
- Avoid discussing consumer/member information in public spaces, such as halls, elevators, lobbies, cafeterias, restaurants, lavatories, parking lots or other unsecured public places where the conversation could be overheard. Be alert to possible eavesdroppers (for both in person and phone conversations).

Electronic Devices

ANY electronically stored or transmitted PHI/PII must be held in a protected and secure manner. This includes:

- Physically positioning monitors, laptops, and other screens to minimize viewing PHI/PII by unauthorized personnel or the public.
- Never leaving electronic devices unattended in publicly accessible venues.
- Emailing PHI/PII using a secure-encrypted program and include the HIPAA Privacy Statement.
- Never sharing passwords/IDs or allowing them to be visible to others.

- Using strong passwords to prevent unauthorized access to devices storing PII/PHI by implementing the following settings on your device:
  - Password History: 4 (This prevents the same password from being reused for at least 4 subsequent passwords.)
  - Maximum Password Age: 90 days (Requiring password changes every 90 days.)
  - Minimum Password Age: 0
  - Minimum Password Length: at least 8 characters
  - Complexity Requirements: enabled
- Setting anti-virus software to scan every 12-24 hours and receive automatic updates.
- Configuring your operating system to receive automatic updates
- Enabling network vulnerability scanning and patch management procedures, where applicable
- For any employees working remotely, implementing Multi-Factor Authentication (e.g., PIN, SmartCard, or biometrics) to ensure secure remote access.

Electronic PHI/PII Storage Such As:

- Portable (jump) storage requires a formally documented and justifiable business reason approved by UnitedHealthcare. Note that any such approval will be rare and exceptional. Mere convenience is not a sufficient reason. If approved, encryption software must be installed on the device.
- Virtual (cloud) storage requires a proper Business Associate Agreement in place with the cloud storage provider and adequate security controls maintained. UnitedHealthcare provides a sample template at: https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

Encryption Software:

ALL electronic devices (computers, phones, tablets, etc.) used to transmit or store PII/PHI must have encryption software installed that renders information unreadable, undecipherable, or unusable with a minimum of 256-bit encryption. Password protection is not the same as encryption.

Below is a list of recommended features and functionality the full-disk encryption solution should offer:

- Full-disk encryption (user data, operating system, temporary files, erased files)
- AES-256-bit encryption
- Pre-boot authentication

While UnitedHealthcare does not recommend or endorse any software or technology company, here are some potential resources to assist you with determining how to find the best fit for your situation.

- The National Institute of Standards and Technology (NIST) is a technology agency under the U.S.

Department of Commerce. They have published a guide on their website documenting their recommendations on full-disk encryption for end user devices, such as laptops and desktops.

- Contacting a reputable security company, such as McAfee or Symantec, for assistance in purchasing a compatible full-disk encryption solution.
- Consulting with a certified IT expert at a large retail vendor that specializes in electronics to assist you with choosing software that is compatible with your device and meets the required standards.
- Software examples includes Windows BitLocker, McAfee Complete Data Protection, Symantec Endpoint Protection.

Note that UnitedHealthcare does not provide technical support in evaluating software to suit your needs.

Retention and Disposal of Enrollment Applications

Retain paper enrollment applications only long enough to verify receipt by the Enrollment Department. (Track status on Jarvis or your commission statement as appropriate.). Securely destroy paper enrollment applications.

Managing Consumer PII/PHI Exposures

All UnitedHealth Group employees, contracted workers, and business associates (including agents) have a responsibility to report any potential or actual inappropriate disclosures or uses of consumer or member PHI.

Examples of inappropriate disclosures include but are not limited to:

- **Misdirected information**: sending an email, fax or hard copy document containing member/customer information to someone other than the intended recipient.
- **Inappropriate disposal** of PII/PHI (e.g., failing to shred paper enrollment application prior to disposal).
- **Lost or stolen hard copy information**: loss or theft of hard copy documents containing member/customer information.
- **Lost or stolen devices containing PII/PHI:**
  - If an unencrypted device containing member/customer information is lost or stolen, such loss or theft could result in an unauthorized/ inappropriate disclosure**.**
  - If your laptop is encrypted with a full-disk encryption program, this type of loss or theft would not be considered an unauthorized disclosure.
- **Discussing member/customer information in public settings**, such as in a restaurant or on an elevator.
- **Discussing member/customer information with friends or family.**

Report incidents of unauthorized or inappropriate disclosures through any one of the following:

- UnitedHealthcare Privacy Office at uhc_privacy_office@uhc.com
- Distribution Compliance at Compliance_Questions@uhc.com
- The UnitedHealth Group Ethics & Compliance Help Center at 1-800-455-4521 or online at https://secure.ethicspoint.com/domain/media/en/gui/13549/index.html

Agents Licensed and Appointed to Sell in New York State

The state of New York periodically sends notifications to agents who are licensed and appointed to sell in that state to certify their compliance with the state's cyber security standards.

Employee agents (ISR channel) are covered under UnitedHealthcare's cybersecurity measures. However, contracted agents are responsible for ensuring that they utilize appropriate cyber security measures for devices they own and operate to do business on behalf of UnitedHealthcare.

UnitedHealthcare does not manage the filing of notices of compliance or exemptions for agents. Agents are expected to determine the applicability of the regulation for their circumstances.

You can visit https://www.dfs.ny.gov/industry_guidance/cybersecurity for more information about New York Cybersecurity Regulations.

Contracted agents needing additional assistance, may wish to seek personal legal counsel.

Additional Resources

If you should like to learn more about HIPAA, we encourage you to review the information found on the HHS website here: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

Agent Guide

The Agent Guide, available on **Jarvis**, provides guidance on CMS regulations and UnitedHealthcare rules, policies, and procedures.

Sales Policy Job Aids (available on **Jarvis**)

Agent Created and UnitedHealthcare Toolkit Materials Guidelines Job Aid

Agent Events Job Aid

Agent Website and Social Media Guidelines Job Aid

Permission to Contact and Lead Generation Job Aid

Prescription Drug Coverage Reference Job Aid

Scope of Appointment Job Aid

Compliance Questions

Submit compliance-related questions to compliance_questions@uhc.com.

Jarvis

Access **Jarvis** through www.uhcjarvis.com.

For assistance accessing or using Jarvis, contact the Producer Help Desk (PHD) at phd@uhc.com or 1-888-381-8581 Mon - Fri 7am - 9pm CT. The PHD also provides agent support with technical issues (navigating UnitedHealthcare's platforms), contracting, certifications, and commission status.