Data Security for Customer Information

Carriers and their agents have a responsibility to protect customer data. In other words, it's the right thing to do. It's also the law: there are federal and state regulations that require carriers and their agents to implement reasonable and appropriate security measures to ensure Protected Health Information (PHI) and Personally Identifiable Information (PII) is protected from unauthorized access, use and disclosure. In order to comply with these various laws, and as part of ongoing efforts to ensure protection of customer data, we will be asking you to confirm that your computer equipment and practices are compliant with certain security standards, where applicable. Here are some of the areas we will be covering as part of this process:

1. Protections for Remote Access of Your Computer Network: You are required to have multiple levels of authentication before allowing anyone to enter the network. To meet this standard your system must use at least two factors to confirm identity before anyone can enter the network. For example, in addition to their password and username combination, anyone trying to enter the network is asked to verify their identity with something that they – and only they — know, such as PIN or a Token Code. Multi-factor authentication should be implemented to authorize anyone requesting remote access – including all third parties (including vendor access for support and maintenance) to prevent unauthorized users access to the organization's internal network where PHI or PII is located.

2. Password Management: Organizations must ensure that all users have a unique user ID and password assigned and that IDs and passwords are not shared amongst users. Group or shared accounts represent significant security and compliance risks from intentional, accidental, or indirect misuse of shared privileges. A unique verifiable user ID shall be assigned to every user in order to establish audit trail & accountability for individual user actions. Passwords for accessing your computers and networks must be encrypted. All passwords should be encrypted at rest, during transmission across the internet, and during transmission over and across the internal network to prevent compromised user accounts.

3. Disk Encryption: Any computer (server, desktop or laptop) that has PHI or PII must implement full disk encryption. Full Disk encryption uses software or hardware to encrypt every bit of data that goes on a disk or disk volume. Full disc encryption helps secure important information and prevents breaches by encrypting all of the data on a hard drive at rest. Without the proper authentication key, even if the hard drive is removed and placed in another machine, the data remains inaccessible.

4. Location Security: You are required to provide a secure physical environment for areas that contain servers, desktop or laptops that have PHI or PII to ensure that only authorized personnel are allowed access. Such measures include locked doors, security cameras, and similar measures to ensure that only authorized personnel are allowed access to servers and critical hardware. Without such controls, unauthorized individuals may gain physical access to systems or areas containing customer data.

5. USB Port and Removable Media Security: You are required to protect your systems and data from attacks through removable media including USB ports. You must have policies and procedures to manage the use of removable storage media, including: identifying those individuals who are permitted to use removable storage devices; describing how such usage and access is monitored and tracked; and, encrypting any removable media that contain PHI or PII. Controls should be in place to assure secure storage of protected information on removable

media like flash drives, discs, or similar media. These devices can be misplaced or stolen resulting in unauthorized data loss or disclosure.

6. System Monitoring: You are required to monitor your computers and systems to protect against, and uncover any hacking of operational systems or files. This monitoring should include:

    a. File integrity checking tools to ensure that critical system files related to protected information (including sensitive system and application libraries, and configurations) have not been altered. Such tools allow the organization to identify any unauthorized changes to system or user files.
    b. Controls to ensure that logging systems and log information are protected from tampering and unauthorized access. Such controls ensure that only authorized individuals can access logs generated from user activities such as login, logout, file read, file write, etc.
    c. Configuring information systems (Domain Controllers, firewalls, switches, routers, Digital Video Recorder-DVR, Building Management System-BMS, anti-virus servers, patch management servers etc.) to receive time updates (Network Time Protocol-NTP) from industry accepted time sources. This activity synchronizes all participating computers to within a few milliseconds and assists in tracking unauthorized access to systems.
    d. System vulnerabilities identified during periodic vulnerability scans are required to be patched as per industry security standards in timely manner.

7. Ongoing Risk Assessment: Finally, you are required to perform risk assessments to identify and quantify risks and communicate the results to management and appropriate third parties on an ongoing basis. New threats to data are constantly emerging, and require ongoing vigilance. Please remember that any material breach to your systems that contain PHI or PII must be reported to UnitedHealthcare immediately.

We look forward to working with you to help assure that customer data remains as secure as possible. We will contact you with further information. In the meantime, please email UnitedHealthcare's Vendor Management Office at uhc_vendor_mgmt@uhc.com with any questions. Thank you for your attention to this important topic.