Buchalter
CLIENT ALERT

October 6, 2021

HIPAA Compliance Guidelines for Remote Workers

By: Jennifer Guerrero

While a remote work environment can provide many benefits to all of the parties involved, it also can present significant challenges for organizations that need to remain Healthcare Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) compliant. There are many privacy and security measures that need to be implemented in order to address the concerns and risks of maintaining HIPAA compliance in a work-from-home environment. This guidance is for educational purposes only and is limited to organizations that are subject to HIPAA and HITECH and is intended to supplement, and not replace the organization's compliance program.

BACKGROUND

HIPAA/HITECH Requirements

HIPAA compliance involves fulfilling the requirements of HIPAA, its subsequent amendments, and any related legislation such as HITECH. Generally, despite the intentionally vague HIPAA requirements, every Covered Entity and Business Associate that has access to PHI must ensure the technical, physical and administrative safeguards are in place and adhered to, that they comply with the HIPAA Privacy Rule in order to protect the integrity of PHI, and that—should a breach of PHI occur—they follow the procedure in the HIPAA Breach Notification Rule.

HIPAA Privacy Rule

The HIPAA Privacy Rule governs how PHI can be used and disclosed. In force since 2003, the Privacy Rule applies to all healthcare organizations, the providers of health plans (including employers), and healthcare clearinghouses and—from 2013—the Business Associates of covered entities. The Privacy Rule demands that appropriate safeguards are implemented to protect the privacy of Personal Health Information. It also sets limits and conditions on the use and disclosure of that information without patient authorization.

HIPAA Security Rule

The HIPAA Security Rule contains the standards that must be applied in order to safeguard and protect electronically created, accessed, processed, or stored PHI (ePHI) when at rest and in transit. The rule applies to anybody or any system that has access to confidential patient data. In this case "access" is interpreted as having the means necessary to read, write, modify, or communicate ePHI, or any personal identifiers that could reveal the identity of an individual. There are three parts to the HIPAA Security Rule—technical safeguards, physical safeguards and administrative safeguards.

APPLICATION IN A REMOTE ENVIRONMENT

While all of the HIPAA/HITECH requirements are applicable in both an in-person and remote setting, the HIPAA information technology (IT) Compliance comes to the forefront in ensuring the remote environment is just as secure as the workplace.

HIPAA IT compliance is primarily concerned with ensuring all the provisions of the HIPAA Security Rule are followed and all elements on your HIPAA IT compliance checklist are covered.

Risk assessment and management is a key consideration for HIPAA IT security. One way to help ensure risks are identified and appropriate controls are implemented as part of your HIPAA IT compliance program is to adopt the NIST Cybersecurity Framework or SOC II compliance standards. Both of these compliance standards are focused in mitigating the risk of data breaches, and implementing appropriate safeguards to detect and respond to attacks in a HIPAA compliant manner when attacks do occur.

HIPAA IT compliance concerns all systems that are used to transmit, receive, store, or alter electronic protected health information. Any system or software that 'touches' ePHI must incorporate appropriate security protections to ensure its confidentiality, integrity, and availability.

Here are some of the steps and guidelines we suggest when you or your employees are outside the office:

I. **Evaluation of Current State**. No one-size-fits-all template exists for privacy programs. For example, the privacy considerations differ for a company operating in 30 states versus a small medical practice operating only in California. When a company begins the process of developing a privacy program, it should develop a basic understanding of certain key considerations that drive the program's nature, structure, and focus. To guide the process at the outset, a company should perform the following to understand and identify the privacy requirements:

1. **Data Mapping:** To properly approach compliance, a business must thoroughly understand the types of personal data it collects and stores. For a new privacy program, an initial project should be to locate the data or create a data map. Specifically, data mapping of all remote employees, source of each data element, data storage locations and format, data usage, data retention, level of access, flow of data. Once the data is mapped, this will need to be reviewed and validated. Understanding the data will help guide the organization to understand any system or application vulnerabilities and where additional safeguards need to be implemented.

2. **Performance of a Risk Assessment:** A risk assessment is a key tool for determining where systems may be vulnerable to a data privacy incident. The risk assessment process identifies the company's unique risk profile, which in turn forms the essential foundation for the company's privacy program. Companies frequently engage third-party vendors for their risk assessments, though some companies may perform risk assessments using qualified internal personnel. A risk assessment generally examines:
    - Threats to the business and its data.
    - Vulnerabilities of the business that may be exploited.
    - The likelihood of any given threat occurring.
    - The harm that may result if any given threat occurred.

Some risk assessments solely examine IT systems. Others look at the fuller picture and take into account:

- Access controls.
- Internal policies and practices.
- Other compliance measurements.

3. **Develop a Compliance Roadmap:** Once the company understands its data, data flows and primary risks, it can create a roadmap towards compliance which considers the risks to be mitigated (prioritized high, medium, low), cost of implementation (focus on high priorities), and timelines to achieve each goal and identification of any easily addressable tasks.

II. **Remote Workforce Specific Compliance Recommendations.** In addition to general HIPAA/HITECH Compliance, here is a list of considerations and recommendations that should be addressed specifically when allowing employees to work from home.

1. **Formalize Work from Home and Remote Work Policies:** Once the company understands its data, data flows and primary risks it can create a roadmap towards compliance which includes development and implementation of the following policies:

   a. Internal policies and procedures that govern how the company collects, uses, protects, retains, and shares personal information and protected health information remotely.

   b. Internal policies and procedures addressing the following:

      i. Prohibit non-employees (friends, family, etc.) from using any devices that contain PHI.
      ii. Require employees who store hard copy (paper) PHI in their home office need a lockable file cabinet or safe to store the information.
      iii. Require employees to destroy any paper PHI once it is no longer needed. The company should also create a policy to specify when it is ok to dispose of any paper records.
      iv. Require employees to follow the organization's media sanitization policy for disposal of all PHI or devices storing PHI.
      v. Require employees to disconnect from the company network when they are done working. Usually, IT configuring timeouts take care of this.
      vi. Prohibit employees from copying any PHI to external media not approved by the company. This includes flash drives and hard drives. You may require all PHI to stay on the company network.
      vii. Mandate that any employees in violation of these procedures will be subject to the company's sanction policy and/or civil and criminal penalties.

   c. Keep logs of remote access activity, and review them periodically. IT should disable any accounts inactive for more than 30 days.

   d. Establish a sanction policy that penalizes employees for violating internal policies and procedures.

e. Create and require each employee sign a Confidentiality Agreement to assure the utmost privacy when handling PHI.

f. Create a Bring Your Own Device (BYOD) Agreement with clear usage rules.

2. **Implement Equipment, Software, and Hardware Requirements:**

a. Establish VPN and require all remote employees or employees who have remote access to use VPN.

b. Establish capability for employees who have access to PHI to encrypt PHI when transmitting PHI and require such encryption for all transmissions. This could be accomplished by restricting all transmissions to be done through a secure portal or software or encryption software incorporated into the email platform.

c. Utilize multi-factor authentication on all platforms that are remotely accessible (if not possible, require strong passwords that must be updated/changed at regular intervals and auto log off from network due to inactivity).

d. Ensure that all laptops remotely accessing the network are equipped with firewalls and antivirus software to protect network access.

e. Restrict use of personal devices for network access unless an employee enters into a bring your own device agreement which outlines usage restrictions and requires the same security and configuration as company issued equipment.

f. Require all devices which are utilized for network access to be encrypted and password protected for access.

g. Ensure all equipment/devices used for network access is properly configured by IT.

Jennifer Guerrero
Attorney
(213) 891-5283
jguerrero@buchalter.com