COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Patient Privacy and Security: Hybrid Work Environment

By Sheila Price Limmroth,[1] CHC, CIA

What Is a Hybrid Work Environment and Its Effect on Patient Privacy and Security?

Traditionally, employers have set expectations that employees physically show up at an office to perform their work assignments. Even jobs that could lend themselves to remote work had in the past required an in-person presence. In 2020, however, such workforce expectations changed with the onset of the COVID-19 pandemic. That summer, Owl Labs and Global Workplace Analytics (GWA) surveyed 2,025 full-time workers in the United States between the ages 21 and 65 at companies with 10 or more employees. The survey found that 80% of respondents expected to work from home at least three days per week after COVID-19 restrictions lifted and workplaces reopened.[2] While we do not know what the future holds, in 2023 many healthcare organizations continued to offer employees hybrid opportunities with administrative services and office work components, allowing employees to work not just from their homes but also remotely in addition to the traditional office.

Working in a hybrid environment requires collaboration and communication technology. Employees must have the tools to be productive from wherever they are working when not in the traditional office setting. An organization may provide equipment that meets the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (e.g., a company-owned cell phone, encrypted computer, or tablet, a secure connection via a VPN, etc.). Some organizations may permit employees and contractors to use their own equipment but require safeguards to protect the data accessed by the home computer and personal mobile devices, as well as any hardcopy materials related to office work. The organization should provide processes employees can follow to safeguard electronic information accessed from outside the organization. In 2021, a report on a Webex by Cisco survey of 2,366 knowledge workers noted that 57% of workers expect to be in the office 10 days or fewer each month and 98% believe future meetings will include remote participants.[3] Thus, setting expectations and compliance controls for hybrid workers is imperative in protecting the organization's data.

A hybrid work environment can create positive goodwill and loyalty for employees looking for work-life balance. In the healthcare arena, a hybrid work environment can also pose significant risk for employers who must comply with HIPAA and state privacy rules. Employers must emphasize patient privacy and their health information, protect personally identifiable information (PII), guard against security risks inherent in the hybrid working environment, and provide guidance and training to employees on how to avoid the risks. In the healthcare arena, it is imperative that patient privacy is protected by maintaining the confidentiality of protected health information (PHI). PHI refers to individually identifiable health information, including demographic data, related to the past, present, or future physical or mental health or condition; the provision of healthcare to an individual; or the past, present, or future payment for such healthcare, which is created or received by the covered entity.[4] This article mainly focuses on risks to PHI in the healthcare setting when employees are working remotely and how the risks can be mitigated through privacy protections and administrative, technical, and physical safeguards listed in the HIPAA Security Rule.

Healthcare Workers and the Hybrid Work Environment

Remote workers with access to PHI may create significant risks for the covered entity. The risks are not limited to electronic PHI (ePHI); paper documents carried back and forth can pose risks, as can verbal conversations in the home office or "on the go." In the past, the typical remote worker in the healthcare setting was the medical records coder. With the COVID-19 pandemic, the dynamic changed, and additional types of healthcare workers now find themselves enjoying the benefits of remote or hybrid work. Because of the pandemic, the typical hybrid worker in the healthcare setting may be accessing billing information, working with customer/patient complaints and grievances, performing quality improvement audits, or coordinating patient care upon discharge. These tasks and others not listed involve significant use of PHI combined with verbal conversations, and, in some instances, print capability. PHI risks are increased with the new tasks that are completed outside the entity's physical building.

The risks that medical information is unsecured increases when employees are no longer in the office where both paper and electronic information can typically be contained through supervision and appropriate processes. Unsecured PHI is subject to breach risk, and the reporting of a breach that is necessary to individuals and the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) has several potential negative ramifications, including reputational harm for the organization. Risks should be assessed for the hybrid work environment so that they may be addressed to prevent security incidents and avoid a breach.

Risk Area Governance

The HIPAA Security Rule and Privacy Rule apply if employees who work remotely have access to PHI as defined in the Privacy Rule. HIPAA describes what should be protected through the Privacy Rule and specifically addresses safeguards necessary for ePHI in the Security Rule.

HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164 (Subparts A and E)

The HIPAA Privacy Rule applies to individually identifiable health information held or transmitted by a covered entity (provider, health plan, healthcare clearinghouse, or business associate) in any form or media, whether electronic, paper, or verbal. This information is called protected health information (PHI). According to the OCR, "'*Individually identifiable health information*' is information, including demographic data, that relates to:

- "the individual's past, present or future physical or mental health or condition,
- "the provision of health care to the individual, or
- "the past, present, or future payment for the provision of health care to the individual,

"and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.13 Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number)."[5]

HIPAA Security Rule, 45 C.F.R. §§ 160, 164 (Subparts A and C)

The HIPAA Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in *electronic* form. The Security Rule calls this information "electronic protected health information" (ePHI). The HIPAA Security Role focuses on the confidentiality, integrity, and availability of ePHI. Confidentiality means the ePHI is accessible only by authorized people; integrity means the ePHI is not altered or destroyed in any unauthorized manner; and availability means ePHI can be accessed as needed by an authorized person.[6]

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. "The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."[7] However, the Security Rule protects ePHI, specifically, covered entities must comply with all of the following:

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit.
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information.
3. Protect against reasonably anticipated, impermissible uses or disclosures.
4. Ensure compliance by their workforce.[8]

Covered entities must determine how they will address the administrative, technical, and physical safeguards described in the HIPAA Security Rule when permitting a hybrid work environment in which the remote worker has access to ePHI.

Office for Civil Rights Guidance on Remote Use

In 2006, the OCR recognized the need for guidance for remote workers with access to ePHI. In the guidance, the OCR states that a covered entity, when deciding on security strategies, should consider the size and complexity of the organization, its technical infrastructure, costs of security measures, and probability and criticality of potential risks to ePHI.

The OCR suggests significant emphasis should be placed on three areas of compliance:

1. Risk analysis and risk management
2. Policies and procedures for safeguarding ePHI
3. Security awareness and training on the policies and procedures[9]