What HIPAA Privacy and Security Considerations Apply to Health Plan Employees Working From Home?

Topic(s): HIPAA Portability, Privacy & Security

QUESTION: Our company sponsors a self-insured health plan. Many plan functions are administered by a TPA, but employees in our benefits department also access protected health information (PHI) when dealing with the TPA and participants. Most of these employees are now working from home due to COVID-19. What HIPAA considerations apply to them?

ANSWER: Remote work can provide significant advantages—and in circumstances like the COVID-19 emergency may be essential—but it also creates privacy and security challenges. The HIPAA privacy and security rules apply to PHI used, disclosed, created, received, maintained, or transmitted by employees of covered entities and business associates, regardless of where the employees are located. All the HIPAA policies and procedures that you follow in an office environment apply equally to employees working from home. However, the policies and procedures may need to be adapted to address additional vulnerabilities created by remote work. Coordination with your multidisciplinary team of IT, legal, HR, operations, and other professionals will help mitigate risk.

With respect to the privacy rule, remember that PHI is broader than diagnosis and treatment information—it includes demographic information such as participants' addresses, phone numbers, email addresses, and financial information, as well as information about their participation in the health plan. Employees should have private workspaces, where conversations involving PHI cannot be overheard by others. They should never access PHI on shared devices and ideally will use only company-issued devices. Hard copies of PHI should be stored in a locked filing cabinet or should be shredded if they cannot be stored securely.

Regarding the security rule, your company's risk analysis and risk management plan should already address remote work, but a substantial increase in the number of remote employees would likely be viewed as an operational change requiring re-evaluation of threats and vulnerabilities and appropriate safeguards. The risk management plan should address the three prongs of the security rule. Some considerations under each prong include—

- *Physical Safeguards.* Although the security rule applies to electronic PHI, physical safeguards are still important. The company should track the location of each computer accessing PHI. Lost or stolen computers may result in unauthorized disclosure of large amounts of PHI, so making sure employees keep them in a secure room is crucial. Employees should also be required to report loss or theft immediately. Devices should never be left unattended in a vehicle or in a public space. Employees may be tempted to write down passwords and keep them near their computer; this practice is as unacceptable when working remotely as it would be on the company's premises.

- *Technical Safeguards.* Controlling access is key, including restricting access to the minimum-necessary PHI for each employee's job function, requiring unique user IDs and passwords, implementing automatic log-off or screen-lock, and utilizing robust encryption tools. Employees should avoid downloading and storing PHI directly on their computer—an individual machine often has weaker protection than a network, and cloud storage may be more secure. Be aware that portable storage media of uncertain provenance may introduce malware onto an employee's computer.

- *Administrative Safeguards.* Procedures should be implemented to supervise remote employees. In addition, logins and information system activity should be routinely monitored to identify security incidents, such as exfiltration of large data files. Remote work will be new to many employees, so mandatory training should be provided on the company's policies and procedures. If remote work results in hiring new service providers, you will need to consider whether business associate contracts are required.

Even with heightened awareness and safeguards, the nature of remote work increases the possibility of unauthorized uses or disclosures of PHI. Because the breach notification rules continue to apply and penalties can be assessed if breach notification is inadequate or untimely, employees should be trained to recognize and promptly report possible breaches.

For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections XXIII.N ("HIPAA Privacy and Security Issues for Employers Whose Employees 'Telework'"), XXV ("Breach Notification for Unsecured PHI"), and XXX ("Core Security Requirements").

Contributing Editors: EBIA Staff.

END OF DOCUMENT -