BURR ARTICLE
BURR FORMAN
2018

Physical Security of Electronic Devices

By Kelli Carpenter Fleming July 2018

Reprinted with Permission from the ***Medical Association of the State of Alabama***

In the age of electronic medical records and ransomware attacks, recent focus with regard to HIPAA compliance seems to be on electronic security. How are your electronic medical records stored? Do you require two-factor authentication to access your electronic system remotely? What firewalls and malware detection systems do you have in place to prevent a cyber-attack?

However, in the May 2018 OCR Cyber Security Newsletter, the Office of Civil Rights ("OCR") reminded providers that, in the midst of electronic security, appropriate physical security controls are also an important component. The HIPAA Security Rule requires that all "workstations" (including laptops, desktops, tablets, smart phones, and portable electronic devices) accessing PHI must have physical safeguards in place to restrict access to authorized users.

According to OCR, the following methods may be helpful in achieving compliance with this requirement: privacy computer screens, cable locks, port and device locks (preventing access to USB ports or removable devices), positioning work screens in a manner in which they cannot be viewed, locking rooms that store electronic equipment, security cameras and security guards. Of course, which methods are appropriate for each provider will vary based on the provider's risk analysis and risk management process.

In reviewing the physical security of electronic devices, OCR recommends that providers ask the following questions:

- Is there a current inventory of all electronic devices (*i.e.*, computers, portable devices, and electronic media) including where such devices are located?
- Are any devices located in public areas or other areas that are more vulnerable to theft, unauthorized use, or unauthorized viewing?
- Should devices currently in public or vulnerable areas be relocated?
- What physical security controls are currently in use (*i.e.*, cable locks, privacy screens, secured rooms, cameras, guards, alarm systems) and are they easy to use?
- What additional physical security controls could be reasonably put into place?
- Are policies in place and employees properly trained regarding physical security (*i.e*., use of cable locks and privacy screens)?
- Are signs posted reminding personnel and visitors about physical security policies or monitoring?

A copy of the May 2018 OCR Cyber Security Newsletter is available here.

For more information, please contact:

Kelli Carpenter Fleming
Partner, Birmingham Office
P. (205) 458-5429
E. kfleming@burr.com