# HHS Office for Civil Rights in Action

## May 2018 OCR Cyber Security Newsletter

### *Workstation Security: Don't Forget About Physical Security*

Physical security is an important component of the HIPAA Security Rule that is often overlooked. What constitutes appropriate physical security controls will depend on each organization and its risk analysis and risk management process.

For HIPAA covered entities and business associates, the Security Rule requires the "[implementation of] physical safeguards for all workstations that access ePHI to restrict access to authorized users."[1] Although this Security Rule standard specifically references "workstations," the term is defined in the HIPAA Rules as "a computing device, for example a laptop or desktop computer, *or any other device that performs similar functions* [emphasis added] and electronic media stored in its immediate environment."[2] Portable electronic devices are included in this definition[3] which could include tablets, smart phones, and similar portable electronic devices.

Many reliable physical security controls are available at little or no cost. For example, privacy screens to prevent someone from viewing your computer screen or cable locks to deter theft can typically be purchased for $20 to $40. Port and device locks that physically restrict access to USB ports or devices such as CD/DVD drives are also available at low costs (technical controls including Microsoft Windows Group Policy configuration and third party software can also be effective at restricting access to USB ports and removable media devices). Unrestricted access to USB ports and removable media devices can facilitate unauthorized copying of data to removable media as well as permit access to removable media which could be infected with malicious software. Cost-free measures include positioning workstation screens away from areas from which they could be viewed, keeping electronic equipment and media in secured areas including locking rooms that store such equipment. Some organizations might also deploy security cameras and guards and post signs accordingly.

Questions for organizations considering a physical security strategy can include:

- Is there a current inventory of all electronic devices (i.e., computers, portable devices, 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?

Failure to take reasonable steps regarding physical security may have serious consequences. Investigations by the U.S. Dept. of Health and Human Services Office for Civil Rights (OCR) that have included, among others, potential violations of the Security Rule's Workstation Security standard have resulted in settlement payments by covered entities ranging from $250,000 to $3.9 million.[4] For example, in 2015 OCR resolved an investigation arising from a breach of PHI involving a laptop used in connection with a computerized tomography scanner that was stolen from an unlocked room.[5]

While the latest security solutions to combat new threats and vulnerabilities get much deserved attention, appropriate physical security controls are often overlooked. Yet physical security controls remain essential and often cost-effective components of an organization's overall information security program.

[1] 45 C.F.R. § 164.310(c)

[2] 45 C.F.R. § 164.304

[3] 68 Fed.Reg. 8340

[4] In September 2012, OCR settled with Massachusetts Eye and Ear for $1.5 million. In April 2014, OCR settled with QCA Health Plan for $250,000. In March 2016, OCR settled with Feinstein Institute for Medical Research for $3.9 million. In July 2016, OCR settled with the University of Mississippi for $2,750,000. In all of these cases, 45 CFR 164.310(c), workstation security was a compliance concern.

[5] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lahey.html

**This newsletter should not be construed as a final agency action and is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.*

A copy of this newsletter may be found at https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-may-2018-workstation-security.pdf. OCR's cybersecurity guidance may be found at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

[1] 45 C.F.R. § 164.310(c)

[2] 45 C.F.R. § 164.304

[3] 68 Fed.Reg. 8340

[4] In September 2012, OCR settled with Massachusetts Eye and Ear for $1.5 million. In April 2014, OCR settled with QCA Health Plan for $250,000. In March 2016, OCR settled with Feinstein Institute for Medical Research for $3.9 million. In July 2016, OCR settled with the University of Mississippi for $2,750,000. In all of these cases, 45 CFR 164.310(c), workstation security was a compliance concern.

[5] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lahey.html