August 2018 Cyber Security Newsletter

Considerations for Securing Electronic Media and Devices

Electronic devices and media play an essential role in the operations of many organizations – including healthcare organizations. Electronic devices can include a broad range of hardware such as laptops, smartphones, servers, desktops, and tablets. Electronic media includes electronic storage devices, such as hard drives, USB drives, CDs/DVDs, tapes and memory cards. These devices and media are used by many organizations to process, transmit, and store sensitive information - including protected health information (PHI). Because of this, organizations should consider what appropriate safeguards are necessary to ensure that the information they handle is secure and their functionality is not impaired.

Many electronic devices and media are used to process or directly store PHI. Anyone with physical access to such devices and media, including malicious actors, potentially has the ability to change configurations, install malicious programs, change information, or access sensitive information – any of these actions has the potential to adversely affect the confidentiality, integrity, or availability of PHI. HIPAA covered entities and business associates are required to implement policies and procedures to limit physical access to its electronic information systems and the facility(ies) in which they are housed. *See* 45 CFR § 164.310(a)(1). Ensuring that only authorized personnel have physical access to its electronic information systems – including hardware, software, information, data, applications, and communications - reduces the risk of physical access by malicious actors. *See definition of information system at* 45 CFR § 164.304. Covered entities and business associates are also required to implement policies and procedures that govern the receipt and removal of hardware and electronic media containing electronic PHI (ePHI) into and out of an organization's facility and their movement within a facility. *See HIPAA Security Rule,* 45 CFR § 164.310(d)(1).

Implementing processes to govern the movement of electronic devices and media may vary depending on the type of device and media. For example, once installed, an organization may not need to move or relocate a server or desktop computer for the entirety of its lifecycle within the organization. Alternatively, portable electronic devices and media like smartphones, tablets, laptops, USB thumb drives, and CDs/DVDs are designed to be highly mobile and may move frequently into, out of, and within an organization's facilities. Portable devices and media thus present an added challenge as they are more susceptible to theft and loss.

To reduce the risk of loss, theft, and the potential of a breach of PHI, organizations may want to consider the following questions when developing policies and procedures regarding device and media controls:

- Is there a record that tracks the location, movement, modifications or repairs, and disposition of devices and media throughout their lifecycles? *See* 45 CFR §§ 164.310(a)(2)(iv), 164.310(d)(2)(i), 164.310(d)(2)(iii); *see also Security Series: Security Standards: Physical Safeguards,* linked below.

- Does the organization's record of device and media movement include the person(s) responsible for such devices and media? *See* 45 CFR § 164.310(d)(2)(iii); *see also HIPAA Security Series: Security Standards: Physical Safeguards* at 12*,* linked below.
- Are workforce members (including management) trained on the proper use and handling of devices and media to safeguard ePHI? *See* 45 CFR § 164.308(a)(5).
- Are appropriate technical controls, for example, access controls, audit controls, and encryption, in use? *See* 45 CFR § 164.312.

Organizations can use a variety of methods to govern and track the movement of electronic devices and media. *See* 45 CFR § 164.306(b). For instance, small organizations with fewer assets may be able to use manual processes whereas larger organizations may use specialized inventory management software and databases. Some inventory management solutions can be used in conjunction with a bar-code system or radio frequency identification (RFID) tags to quickly organize and identify devices and media. These systems may allow for easier, quicker, and more accurate tracking and verification of implemented controls. An organization's risk analysis and risk management processes should guide it to identify and implement appropriate device and media controls. *See* 68 Fed. Reg. 8334, 8341 (Feb. 20, 2003). Additionally, when determining what security measures to implement, covered entities and business associates must consider the following factors (*See* 45 CFR § 164.306(b)(2)):

- Its size, complexity, and capabilities.
- Its technical infrastructure, hardware, and software security capabilities.
- The costs of security measures.
- The probability and criticality of potential risks to ePHI.

During the lifecycle of an asset, there will be a point at which an organization wishes to reuse or dispose of the asset. HIPAA covered entities and business associates must ensure that devices and media containing PHI that are scheduled for redeployment or final disposition undergo appropriate reuse or disposal processes to ensure that PHI stored on such devices and media cannot be retrieved. For additional information on device and media disposal and reuse please see OCR's July 2018 cybersecurity newsletter, *Guidance on Disposing of Electronic Devices and Media*, linked below.

Additional Benefits

Implementing appropriate controls for devices and media can help an organization comply with other provisions of the Security Rule. *See, e.g.*, 45 CFR §§ 164.308(a)(1), 164.308(a)(6). HIPAA covered entities and business associates are required to have a security management process in place which includes conducting a risk analysis and implementing a risk management process to reduce risks and vulnerabilities. See 45 CFR §§164.308 (a)(1)(ii)(A)-(B). Asset inventory and tracking can help organizations identify, analyze, and manage the risks associated with devices and media used within their environment.

Device and media controls can also help organizations respond to, and recover from, security incidents and breaches. Accurate tracking and proper implementation of controls may allow organizations to quickly identify what devices and media may be affected by an actual or suspected security incident, or breach, and respond accordingly. For example, if hackers gained access to an organization's network by exploiting a vulnerability present in a particular electronic device, or if a particular type of electronic media was identified to include malicious software, a robust and accurate inventory and tracking process could identify how many devices or media are affected and where they are located. With this

information, an organization should be able to make more effective use of its resources and respond more effectively to an actual or suspected security incident or breach involving such devices or media.

For additional resources regarding device and media controls, please see the following resources:

Guidelines for Managing the Security of Mobile Devices in the Enterprise:
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf

Guidance on Disposing of Electronic Devices and Media:
https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-july-2018-Disposal.pdf

HIPAA Security Series: Security Standards: Physical Safeguards:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

* *In general, OCR's newsletters do not establish legally enforceable responsibilities. Instead, these newsletters should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited.*