July 2018 OCR Cybersecurity Newsletter

Guidance on Disposing of Electronic Devices and Media

Because the technology and computer equipment that organizations use may contain components that store sensitive information, organizations should consider whether their process for disposing of electronic devices and media does so in a secure manner. Examples of such computer equipment include desktops, laptops, tablets, copiers, servers, smart phones, hard drives, USB drives, or any electronic storage device.
Storage media used by electronic devices contains various kinds of data, some of which may be sensitive - such as financial information or protected health information (PHI).

What's at Risk? Improper disposal of electronic devices and media puts the information stored on such devices and media at risk for a potential breach. Data breaches can be very costly to organizations. Examples of potential monetary costs incurred as a result of a breach include: notifications; responding to government investigations; lawsuits; hiring of crisis communications or public relations consultants, breach response consultants, legal counsel, and security specialists; and the potential loss of business due to a loss of confidence with customers. Therefore, an organization's risk analysis plays a critical role in determining how best to protect data stored on electronic devices and media that has reached the end of its useful life. To reduce the risk of breaches of data stored on devices or media scheduled for final disposition, organizations may want to consider the following:

- What data is maintained by the organization and where is it stored?
- Is the organization's data disposal plan up to date?
- Are all asset tags and corporate identifying marks removed?
- Have all asset recovery-controlled equipment and devices been identified and isolated?
- Is data destruction of the organization's assets handled by a certified provider?
- Have the individuals handling the organization's assets been subjected to workforce clearance processes and undergone appropriate training?
- Is onsite hard drive destruction required?
- What is the chain of custody?
- How is equipment staged/stored prior to transfer to external sources for disposal or destruction?
- What are the logistics and security controls in moving the equipment?

Devices or media that need to be replaced should be decommissioned and disposed of securely to ensure that either the devices or media are destroyed or any confidential or sensitive information stored on such devices or media has been removed. Decommissioning is the process of taking hardware or media out of service prior to the final disposition of such hardware or media. Steps organizations can consider as part of its decommissioning process include:

- Ensuring devices and media are securely erased and then either securely destroyed or recycled;
- Ensuring that inventories are accurately updated to reflect the current status of decommissioned devices and media or devices and media slated to be decommissioned; and
- Ensuring that data privacy is protected via proper migration to another system or total destruction of the data.

Destruction and Disposal of PHI. The HIPAA Security Rule requires HIPAA covered entities and business associates to implement policies and procedures regarding the disposal and re-use of hardware and electronic media containing PHI in electronic form (ePHI). See 45 C.F.R. §§164.310(d)(2)(i)-(ii). When developing policies and procedures for the final disposition of hardware and electronic media containing ePHI, covered entities and business associates should:

- Determine and document the appropriate methods to dispose of hardware, software, and the data itself.
- Ensure that ePHI is properly destroyed and cannot be recreated.
- Ensure that ePHI previously stored on hardware or electronic media is securely removed such that it cannot be accessed and reused.
- Identify removable media and their use (tapes, CDs/DVDs, USB thumb drives).
- Ensure that ePHI is removed from reusable media before they are used to record new information.

OCR's Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals[1] provides information on how to dispose of PHI securely. PHI disposed of in accordance with this guidance is not considered "unsecured" PHI and, therefore, would not be subject to HIPAA breach notification requirements (see 45 C.F.R. §§164.400-414). PHI is considered to have been disposed of in a secure manner when the media on which the PHI is stored or recorded has been destroyed in one of the following ways:

- Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization[2] such that the PHI cannot be retrieved.

For additional materials regarding secure disposal practices, please consult the following resources:

- https://intranet.hhs.gov/it/strategy-policy-governance/eplc/artifacts/eplc_disposition_plan_practices_guide.pdf
- https://www.us-cert.gov/sites/default/files/publications/DisposeDevicesSafely.pdf
- https://www.nsa.gov/resources/everyone/media-destruction/
- https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html
- https://www.hhs.gov/hipaa/for-professionals/faq/576/may-a-covered-entity-dispose-of-information-in-dumpsters/index.html

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf