KRIEG DEVAULT

Insights

OCR Issues Guidance on Disposing of Electronic Devices and Media

August 9, 2018

By: Stephanie T. Eckerle and Meghan M. Linvill McNab

On August 7, 2018, the HHS Office of Civil Rights (OCR) issued guidance on disposing of electronic devices and media[1]. This guidance is important for all healthcare providers as it applies to any covered entities or business associates that store ePHI on desktops, laptops, copiers, cell phones, USB devices and other electronic storage devices. In addition, OCR's guidance also reminds covered entities and business associates that it is critical to properly dispose of paper records that contain PHI.

The guidance issued by OCR focuses on the following four tasks that covered entities and business associates can undertake to ensure that their PHI as well as electronic devices are disposed of properly: (1) undertaking a thorough risk analysis; (2) properly decommissioning and disposing of devices and media; (3) having HIPAA policies and procedures that address the disposal of devices and PHI; and, (4) properly destroying or disposing of PHI.

Risk Analysis

HHS highlights that one of the first things that a covered entity should ensure is that their risk analysis addresses the PHI stored on electronic devices and media. A few of the questions that covered entities may want to consider when conducting a risk analysis as it relates to the disposal of PHI are as follows:

- 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?
- Is data destruction handled by a certified provider?

Decommissioning of Devices

OCR also focuses on the importance of properly decommissioning devices. Decommissioning is the process of taking hardware or media out of service prior to the final disposal of such hardware or media. HHS highlights the following three steps that covered entities and business associates should take when decommissioning devices:

- 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.

HIPAA Policies and Procedures

The third topic that OCR focuses on is the proper destruction and disposal of ePHI. OCR reminds covered entities and business associates that their HIPAA policies and procedures must address the disposal of ePHI. OCR provides examples of what such policies must contain, such as ensuring that the policies determine and document the appropriate method to dispose of hardware, software and the data itself. In addition, covered entities should also ensure that workforce members who dispose of PHI or supervise others that dispose of PHI receive training on such disposal[2].

Destruction and Disposal of ePHI

Last, OCR focuses on how PHI should be destroyed to ensure that it is not considered unsecured PHI. OCR highlights the following methods:

- Paper, film, or other hard copy media must be 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 must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

Although OCR just issued this Guidance, OCR has actively addressed the issue of failing to properly dispose of PHI in settlements with covered entities as well as multiple other publications. For example, in 2015 OCR entered into a Resolution Agreement with a pharmacy due to the pharmacy's alleged disposing of patient records in a dumpster that was accessible to the public[3]. OCR found that among other things, this pharmacy failed to: (1) reasonably safeguard PHI; (2) implement proper written policies and procedures in compliance with HIPAA's privacy rule; and (3) provide HIPAA training to members of its workforce. This Resolution Agreement as well as other guidance issued by OCR on this topic demonstrate that all covered entities and business associates need to ensure that the proper disposal and destruction of PHI as well as devices containing PHI is a top priority.

Please contact Stephanie T. Eckerle, Meghan M. Linvill McNab or your regular Krieg DeVault attorney with any questions about disposal and destruction of PHI or other HIPAA related issues.

[1] July 2018 OCR Cybersecurity Newsletter, Guidance on Disposing of Electronic Devices and Media, https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-july-2018-Disposal.pdf.

[2] *See* HHS, FAQ for Professionals, What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?, https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html.

[3] Resolution Agreement, United States Department of Health and Human Services, Office for Civil Rights and Cornell Pharmacy, 2015, https://www.hhs.gov/sites/default/files/cornell-cap.pdf; HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records, https://www.hhs.gov/hipaa/for-professionals/compliance-

enforcement/examples/cornell/cornell-press-release/index.html.