MassAHU Members Only Bulletin August 2018

DISPOSING OF ELECTRONIC DEVICES AND MEDIA

This bulletin is about your laptop, smart phone, USB thumb drives (multiplied by the number of the staff members in your office); even your office photocopier(s). These devices can be lost or stolen (hopefully this is less likely for your office photocopier(s)). Perhaps it's just time to replace them because they are old, worn out, or technologically out of date.

Many insurance brokers are considered business associates for HIPAA privacy and security purposes. How much PHI or other sensitive information do you carry on your smart phone alone? What about all the attachments to emails you open on your smart phone containing enrollment information, SSNs, claims issues, lasered claims under a client's stop loss policy just to name a few?

Last month (July 2018) HHS's Office for Civil Rights (OCR) issued general guidance in newsletter form on disposing of electronic devices and media that may contain protected health information (PHI) subject to HIPAA.[*] 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).

The newsletter discusses, generally with references to other OCR documents, that procedures for securely decommissioning and disposing of devices or media that need to be replaced are necessary. In general, these procedures involve either:

- Destroying the devices or media.
- Removing any confidential or sensitive information stored on the devices or media.

The improper disposal of electronic devices and media that are being replaced or updated puts the information stored on them at risk for a potential breach. Data breaches can be very costly to organizations. In addition to costly settlement agreements with OCR, 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.

DESTRUCTION AND DISPOSAL OF PHI

According to the OCR newsletter, devices or media that are being replaced should be decommissioned and then 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

[*] *In general, OCR's newsletters do not establish legally enforceable responsibilities. Instead, these newsletters are guidance documents that describe OCR's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited.*

been removed. Decommissioning is the process of taking hardware or media out of service prior to the final disposition of the hardware or media.

Steps organizations may consider as part of the 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 devices and media that are decommissioned or slated to be decommissioned; and
- Ensuring that data privacy is protected via proper migration to another system or total destruction of the data.

PHI disposed of consistent with HHS guidance is not considered "unsecured" PHI and, therefore, is not be subject to HIPAA breach notification requirements. 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 such that the PHI cannot be retrieved.

RECENT EXAMPLES OF OCR ENFORCEMENT ACTION

A HIPAA breach could result in an OCR investigation followed by enforcement action and settlement agreement. This could result in penalties/fines and even a multi-step corrective action plan that may take months and many resources to implement. HIPAA-related settlements resulting from legal action taken by OCR against entities for data breaches are real. Here are some examples:

- OCR investigated a Texas cancer research and treatment facility following three separate data breach reports in 2012 and 2013 involving the theft of an unencrypted laptop from the residence of a facility employee and the loss of two unencrypted universal serial bus (USB) thumb drives containing the unencrypted electronic protected health information (ePHI) of over 33,500 individuals. Cost to the facility for breach of HIPAA: **$4,348,000 in civil money penalties**
- An insurance company had a USB drive containing protected health information stolen from its IT department in August 2011. Data on the drive included member names, dates of birth and Social Security numbers, affecting 2,209 persons. Cost to the company for the breach of HIPAA: **$2.2 million fine** agreed to in January 2018 in settlement with OCR for violations of the HIPAA privacy and security rules.

- OCR investigated a breach of PHI involving the theft of a company-issued employee iPhone. The company provided management and information technology services as a business associate to six skilled nursing facilities. The iPhone was unencrypted and was not password protected. The information on the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. The total number of individuals affected by the combined breaches was 412 individuals. Cost to the company for the breach of HIPAA: **$650,000 fine** and a corrective action plan.

- A health plan (and HIPAA covered entity) was investigated by OCR and later entered into a resolution agreement to settle alleged violations of HIPAA's privacy and security rules. The health plan notified OCR of a breach involving ePHI after it was informed by a representative of CBS Evening News as part of an investigatory report. CBS news apparently purchased one of several photocopiers previously leased by the health plan and found confidential medical information on the photocopier's hard drive. OCR concluded that the health plan impermissibly disclosed the electronic PHI of up to 344,579 individuals by failing to properly erase photocopier hard drives before returning the photocopiers to the leasing company. Cost to the company for the breach of HIPAA: **$1,215,780 fine.**

* * * * *

This month's bulletin carries the following message -- simply be aware of the issues discussed above when disposing of electronic devices and media that may contain PHI. Disposition could be by charitable donation, internal or external transfer, or by recycling if the media is obsolete or no longer usable. No matter what the final intended destination of the media is, it's important that your organization ensures that no easily re-constructible residual representation of the data is stored on the media after it has left the control of your organization.

Richard A. Szczebak, Esq.
781-731-9933 | rszczebak@raslawpc.com
Experience | Knowledge | Perspective