# OCR Reminds Employers to Follow Proper Steps When Disposing of Electronic Devices and Storage Media

**Issue Date: September 2018**

## Quick Facts:

- The Office of Civil Rights (OCR) recently issued guidance on the dangers inherent in upgrading and disposing of computer equipment and other electronic devices.
- Sensitive information can be subject to data breaches when employers improperly dispose of technological devices.
- Employers should be aware of the type of data they maintain on electronic devices or media.
- Employers – including health plan sponsors – should have protocols in place to properly handle and protect sensitive data like protected health information (PHI) before discarding or repurposing electronic devices and storage media.

## Overview

Businesses have become ever more dependent on technology, and the rate at which that technology becomes obsolete has increased dramatically. Thus, companies frequently face the challenge of upgrading computers and other electronic devices to keep pace with market demands. This process typically involves disposing of electronic devices and storage media. Many employers gift, donate, recycle or even discard the equipment unaware of the serious risk of compromising confidential employee or customer information that is stored on such devices.

## Improper Disposal of PHI

The Office of Civil Rights (OCR), the enforcement arm of the U.S. Department of Health and Human Services (HHS), recently issued a Cybersecurity Newsletter in which it highlighted the dangers inherent in upgrading and disposing of computer equipment and other electronic devices, including laptops, tablets, smart phones, USB drives, and copiers that contain protected health information (PHI), financial and other sensitive information. OCR cautioned HIPAA-covered entities, including employer-sponsored health plans and business associates, to carefully analyze whether they dispose of such equipment securely – guidance HIPAA-covered entities and business associates would be wise to heed given the recent surge in HHS and OCR investigation and enforcement activity.

Improperly disposing of computer equipment and electronic devices that store sensitive information (e.g., health information (PHI) subject to the Health Insurance Portability and Accountability Act [HIPAA]) can put a covered entity at risk for a serious data breach.

***What is PHI? What is ePHI?***

PHI is individually identifiable health information that is created, received, maintained, or transmitted by a HIPAA-covered entity or business associate. PHI in electronic form is referred to as electronic PHI (ePHI).

In addition to potentially harmful negative publicity and loss of goodwill that comes with a major data breach, plan sponsors must also start a complex breach analysis and response that often entails notifying affected individuals, HHS, and the media; as well as engaging crisis management experts, public relations consultants, security specialists, and legal counsel.

## Steps for Reducing Exposure to Data Breaches

Employers and health plan sponsors can greatly reduce their exposure to a serious inadvertent data breach by thoroughly understanding what types of data they maintain and where it is stored, especially when it comes to PHI. Employers that need to dispose of equipment that houses sensitive data should have written policies that detail proper sanitization and disposal. Such policies should require, at a minimum, training applicable employees to identify and carefully handle sensitive data, ensuring the integrity of storage devices (including cloud-based storage), maintaining a chain of custody log on all electronic devices, consider removing any corporate identifying marks, hiring a certified vendor to handle data destruction, and ensuring secure storage or transfer of the devices to that vendor.

OCR has identified the following steps as vital to an electronic device decommissioning and disposal plan:

- Securely erase devices and media.
- Securely destroy or recycle devices and media.
- Properly migrate data to another system or destroy sensitive data altogether.

HIPAA requires covered entities and business associates to implement specific policies and procedures to dispose of or reuse hardware and electronic media containing ePHI. OCR admonishes covered entities and business associates to:

- Determine and document appropriate methods to dispose of hardware, software, and the data itself.
- Ensure ePHI is properly destroyed and cannot be recreated.
- Ensure that ePHI previously stored on hardware or electronic media is securely removed and cannot be accessed and reused.
- Identify removable media (e.g., CDs, DVDs, USB thumb drives) and ensure ePHI is removed before using to record new information.

## OCR Disposal Guidance

Entities that dispose of PHI in accordance with OCR's *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (see link below) will automatically prevent that data from being considered unsecure under HIPAA. The data, therefore, will not be subject to HIPAA breach notification requirements if inadvertently disclosed.

PHI is considered to have been disposed of securely when:

- Paper, film, or other hard copy media has been shredded or destroyed such that PHI cannot be read or otherwise cannot be reconstructed. Redaction is not considered a secure 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* so PHI cannot be retrieved.

## Summary

Employers who face a need to upgrade hardware or media storage devices that contain sensitive data, including PHI, should review their policies and procedures to follow HIPAA requirements and the latest OCR guidance.

Taking the time and the few extra steps needed to develop a compliant set of policies and procedures for disposing of electronic hardware and other media can help avoid the severe and dire consequences of a data breach.

In addition to proper disposal of PHI, covered entities and business associates are required under HIPAA to establish overall policies and procedures regarding the use, disclosure, transmittal and retention of PHI, appoint officials to monitor HIPAA compliance, and conduct workforce training, conduct security risk assessment on systems containing e-PHI, and much more. To request assistance with HIPAA privacy and security rule compliance, please contact a member of your account team.

**Additional Resources**

The following resources provide valuable information on this important topic:

- Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- NIST Special Publication 800-88 – Guidelines for Media Sanitization
- NSA Media Destruction Guidance
- HIPAA Data Disposal FAQ
- EPIC's Archived 2016 Compliance Alert: HHS Guidance Sheds Light on "Cloudy" Situation