COSMOS
Navigate the Compliance Universe

Compliance Today - September 2021
How to properly sanitize electronic media containing PHI

By Michael Harstrick, CSDS

Michael Harstrick (mharstrick@garner-products.com) is the Chief Global Development Officer at Garner Products Inc., Roseville, CA.

- linkedin.com/in/michael-harstrick/

If you look into the IT closets of many healthcare organizations, you will find stockpiles of old hard drives, thumb drives, cell phones, tablets, and laptops waiting. Waiting for what? Many organizations do not know what to do with decommissioned electronic media. This inaction creates a potentially costly risk of protected health information (PHI) data breaches from media loss, theft, and unauthorized resale of media on secondary markets.

Also, think about the fact that all medical monitoring devices store data. Each one puts you at risk of a potential Health Insurance Portability and Accountability Act (HIPAA) violation. Even your leased technology, such as fax machines, copiers, and printers, collect and store PHI that you are responsible for protecting. While organizations are often aware of front-end security threats such as hacking and ransomware, end-of-life media disposal often goes overlooked. Securely and properly disposing of decommissioned hard drives and other electronic media protects your patients' PHI and can keep your organization off the HIPAA Wall of Shame.[1]

How to properly sanitize electronic media of PHI

According to the U.S. Department of Health & Human Services,[2] proper sanitization methods of PHI on electronic media include clearing, purging, and destroying.

Electronic media includes magnetic media, such as hard drives and storage tape, and solid-state media, such as thumb drives and solid-state drives.

Clearing (overwriting)

Clearing uses software to overwrite data on electronic media with nonsensitive data, usually a pattern of 1s and 0s, to write over the underlying data.

Overwriting is a method that allows the media to be reused. However, reuse of overwritten media is only advisable if the media is being reused within the same organization and the media will not be leaving the organization's control. The reason for this restriction is that overwriting is not secure. The media must be 100% functioning for all of the data to be overwritten. If the media has bad sectors or is nonfunctioning, the data cannot be completely overwritten. Unfortunately, there is no way to identify nonworking sectors and, in turn, the success or failure of the overwriting process.

Overwriting is a lengthy process. It takes between 8 and 14 hours of continuous writing by a skilled operator to overwrite a drive that is in good condition. Older or worn-out media can simply fail, leaving unwritten PHI data on the media. Plus, it usually takes multiple passes—three is recommended—to erase the drive, but many operators often make only one pass, leaving the PHI vulnerable to a breach.

Purging (degaussing)

Purging, also called degaussing, sanitizes magnetic media (i.e., hard drives and storage tape) of all data regardless of whether the media is working or nonfunctioning. In just seconds, the strong magnetic pulse from a degausser encompasses the media, completely eliminating all magnetic field patterns and, in turn, all PHI on the media.

Degaussers, about the size of a CPU, plug into a standard wall outlet and are designed to be used in an office environment by office personnel without any specialized training. Degaussing has proven to be the most thorough, time-efficient, and cost-effective process for sanitizing hard drives and storage tapes. By implementing a degaussing protocol, media will not leave its secure facility without first being sanitized of all data.

It is important to note that some degaussed tapes are not usable. However, degaussing renders hard drives unusable, and in those cases, degaussing is also a destruction technique. Degaussing cannot be used on thumb drives and solid-state drives as this type of media contains nonmagnetic microchips that need to be physically destroyed.

Destroying (crushing and shredding)

Although there are many ways to physically destroy media, the most common methods are crushing and shredding.

Crushing devices prevents data recovery by use of force to bend, break, mangle, and puncture electronic media, including the media's data platters, microchips, and other internal components. Many crushing devices are designed for use inside IT departments and office environment so the media can be physically deformed without leaving its secure facility. Particular brands of physical destroyers are small, about the size of a CPU, and plug into a standard wall outlet. Single-button operation makes the equipment easy to use by office and healthcare personnel. Depending on its crush chamber size, crushers will physically deform most types of electronic media. When it comes to hard drives, it is important to note that crushers only deform hard drives, but the PHI data remains unless the drive has been degaussed. For this reason, hard drives must first be degaussed before they are crushed.

Shredding cuts electronic media into two or more pieces, deforming the media in such a manner that thieves will be less inclined to attempt to retrieve the data. Most hard drive shredders are large, heavy pieces of machinery that cannot be brought in-house. Since shredding works for paper, logic assumes that it works for all electronic media as well, which it does for solid-state drives. However, shredding is insufficient for protecting PHI on magnetic hard drives, as a modern hard drive can store 600,000 pages of data on a two-millimeter-wide shred particle. That is a particle smaller than a grain of rice! Like crushing, shredding deforms the media but leaves the PHI on magnetic drives. Magnetic hard drives must first be degaussed before they are shredded to ensure the data is irretrievable.