Report on Patient Privacy Volume 18, Number 9. September 30, 2018 When Junking Equipment, Devices, Remember That ePHI Will Live On

By HCCA Staff

A few years ago, a medical device researcher bought a pacemaker and related equipment on eBay. Not only did he acquire the device and its controller, says his friend Rebecca Herold, he also got "very detailed patient data of 51 patients…even including doctors' notes about patient visits and evaluations."

Herold relates the experience in light of a recent monthly newsletter issued by the HHS Office for Civil Rights (OCR), "Guidance on Disposing of Electronic Devices and Media." OCR advises that "organizations should consider whether their process for disposing of electronic devices and media does so in a secure manner."

Obviously, whoever had the pacemaker before her friend didn't do the right thing when it comes to erasing electronic protected health information (ePHI).

OCR's message is one that covered entities (CEs) and business associates (BAs) need to hear, says Herold, president of the HIPAA consulting firm SIMBUS360 and CEO of The Privacy Professor.

Not all CEs and BAs are handling disposal appropriately, and there's sometimes "a mix within the specific organization itself," she tells *RPP*.

Herold says some "do a very good job with disposing of their organization-owned laptops, but then completely overlook the disposal, or decommission, of the laptops that are owned by employees and contractors that are used for business purposes."

The issue is reflected in the quality of entities' plans for disposing of data and media, which Herold says "vary greatly."

While some "have disposal procedures that are multiple pages long and address every type of device and media where data is found," she says, "others simply don't have a documented procedure at all."

And such devices are numerous: think of "desktops, laptops, tablets, copiers, servers, smart phones, hard drives, USB drives," reminds the July OCR newsletter, which was issued in early August.

OCR makes the point—a common refrain from the agency—that a thorough risk assessment is an essential first step in compliance.

Such an 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," it says.