COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 2. February 28, 2018 Newly ID'd Spectre/Meltdown Threat Requires Patches to Nearly All Systems

By HCCA Staff

Spectre and Meltdown—recently discovered vulnerabilities found in nearly all computing devices—could be points of entry for hackers. Therefore, information technology security experts say health care organizations should move swiftly to patch these vulnerabilities, starting with their most critical systems.

At the same time, though, those responsible for security at health care entities should be aware that older systems running on outdated operating systems can't be patched, and patching likely will slow down processing.

"Spectre and Meltdown are dangerous in all spaces, but they introduce an extraordinarily high risk to health care organizations" because of the industry's reliance on technology, says Kathie Miley, chief operating officer at cybersecurity training firm Cybrary, Inc. "As such, if you work in health care IT and are not completely aware of these vulnerabilities, their risks, and don't have a plan to mitigate them, act quickly."

Spectre and Meltdown are two different, but related, vulnerabilities recently uncovered in Intel and other CPUs, which are the brains of computing devices ranging from servers to phones.

In a report released Jan. 5, the Critical Infrastructure Protection (CIP) office of the Office of the Assistant Secretary for Preparedness and Response (ASPR) reported that "a widespread vulnerability in most computer processors sold over the previous decade has been identified that could pose a threat to the protection of Healthcare and Public Health (HPH) sector sensitive data, Protected Health Information (PHI), and Personally Identifiable Information (PII)."

CIP rated the significance of the vulnerability for the health care and public health care sector as medium "due to the fact that local access to the computing device is generally required, and vendors are quickly releasing appropriate software patches to mitigate the hardware vulnerability."