Department of Health and Human Services requires physical security for HIPAA compliance of devices accessing electronic patient health information

In May 2018, the Department of Health and Human Services released clarifying documentation as it relates to HIPAA compliance for workstations and devices that access electronic patient health information (ePHI). The communication, titled Workstation Security: Don't Forget About Physical Security, stresses the notion that physical security as it relates to workstations, as part of 45 C.F.R. 164.310 (C), applies beyond the traditional definition of laptops and desktop computers. The communication extends this definition to any device that accesses ePHI, including smartphones and other portable computing devices.

As the internet of medical things continues to proliferate the healthcare ecosystem, it becomes critical to implement access controls on all devices that interact with ePHI in order to maintain HIPAA compliance. Network-connected medical devices such as patient monitors and infusion pumps are a particular point of concern for many healthcare organizations. Medical devices have become increasingly valuable resources in the delivery of patient care, enabling data to be captured, aggregated, transmitted, and analyzed in real time. However, with these advanced capabilities come new security threats, as each device represents a potential point of exposure of patient information.

Some of the physical security measures suggested by the Department of Health and Human Services, to ensure HIPAA compliance include restricting access to unauthorized users by implementing measures such as:

- Privacy screens for devices used in public areas
- Cable locks to prevent theft of devices
- Restricting access to USB ports and CD drives
- Keeping high risk devices in locked rooms
- Other physical security controls that can easily be put into place

Unfortunately, most network-connected devices, such as medical devices, shared mobile devices, and other devices that support mobility and point of care workflows are difficult to completely secure through the methods listed above. Therefore, other security best practices, such as implementing access controls that require strong authentication, are critical steps in achieving physical security on clinical devices.

To help get started, Imprivata has published a whitepaper, *Best practices: Access controls for medical devices*, which outlines how organizations can begin implementing security measures on connected devices without impeding clinical efficiency.