OCR recommends IT asset inventory for HIPAA compliance

September 9, 2020

The Office of Civil Rights (OCR) recently issued its Summer 2020 Cybersecurity Newsletter to recommend that health care providers and business associates create information technology (IT) asset inventories in order to track where electronic health information (ePHI) is located within their organization. OCR has found that providers frequently do not know where all of their ePHI is located, which creates problems for compliance with risk analysis requirements under the HIPAA Security Rule.

OCR explains that providers should create system-wide IT asset inventories that comprehensively list all of their organization's assets. That list should include sufficient descriptive information to aid in location of ePHI, including identifying asset names and types, software versions, locations and the individual responsible for the asset. OCR specifically recommends that the IT asset inventory include:

- Hardware assets: Physical elements of the organization's networks and systems, including electronic devices and media.
- Software assets: Programs or applications that run on the hardware assets, including databases, email and financial record systems, backup solutions, and anti-malware tools.
- Data assets: ePHI that is created, received, maintained, or transmitted on the network or with the hardware

assets.

IT asset inventories should also consider IT assets that may not be involved in storing or processing ePHI as those assets may still present a method of intrusion into an organization's IT systems.

Understanding where your organization stores ePHI is essential to conducting an accurate and thorough risk analysis as required by HIPAA. OCR's newsletter also notes additional benefits of IT asset inventories, such as compliance with the requirement to track movement of electronic media in and out of facilities. Additionally, IT asset inventories can aid organizations in tracking necessary software updates to devices and compliance with security polices, such as password changes.

Authors

Chris Bennington
Partner

Cincinnati
513.870.6572
cbennington@bricker.com

Joshua M. Gilbert
Senior Associate

Columbus
614.227.7736
jgilbert@bricker.com