Complying with the HIPAA Security Rule for ePHI

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 to regulate the protection of privacy and security of certain health information. The HIPAA Privacy Rule established the national standards for protected health information (PHI), and the HIPAA Security Rule established the national standards for electronic protected health information (e-PHI). The Office for Civil Rights (OCR) enforces both the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

The HIPAA Security Rule allows organizations to adopt new technologies to improve the quality and efficiency of healthcare, while keeping electronic personal health information secure. Organizations in the healthcare industry such as hospitals, healthcare clearinghouses, and organizations that electronically transmit health information are subject to this rule. The searches in this use case enhance the technical safeguards that your organization already has in place to add an extra layer of security for e-PHI. This use case will help your organization be HIPAA compliant to prevent any legal consequences.

Required data

- Endpoint data
- Medical device data

How to use Splunk software for this use case

You can run many searches with Splunk software to help ensure compliance with HIPAA. Depending on what information you have available, you might find it useful to work on some or all of the following:

- Access controls
- Audit controls
- Integrity controls
- Person or entity authentication
- Transmission security

Next steps

Measuring impact and benefit is critical to assessing the value of compliance operations. When implementing this use case, you should track the number of out-of-HIPAA-compliance incidents detected over time. In addition, review compliance office requirements and reporting policies, and have a method of developing and maintaining an asset and identity catalog with in-scope attributes.
In addition, these Splunk resources might help you understand and implement this use case:

- Solution Guide: Splunk for Healthcare
- Blog: New HIPAA and PCI-DSS compliance attestations for Splunk Cloud