A HIPAA compliance cheat sheet

How to maintain compliance with Title II of HIPAA

The importance of secure transactions in healthcare

Compliance violations are minimum $50,000 and up to $1.5 million per year

When the Health Insurance Portability and Accountability Act (HIPAA) was established in 1996, there were no smartphones or wirelessly connected medical devices, and very few care providers stored electronic protected health information (ePHI). But today, communication systems let medical professionals access ePHI via laptop, tablet or smartphone. Biometric data can be collected through wearable devices and shared with physicians or health care insurers. Some ailments can even be treated over video conference.

As all of this happens, hackers spare no effort to pilfer ePHI for gain. Now, more than ever, health care organizations must streamline methods that maintain compliance with Title II of HIPAA. This document serves as a reference for IT decision-makers who seek to facilitate easier HIPAA compliance management.

The Title II checklist

Title II is primarily concerned with secure storage, processing, transfer and access of ePHI and other electronic health care transactions. It is divided into five sub-sections:

1. National Provider Identifier
2. Transactions and Code Sets
3. Standards for Privacy of Individually Identifiable Health Information
4. Security Standards for the Protection of Electronic Protected Health Information
5. HIPAA Enforcement Rule

Sections two through four contain the bulk of the technical and administrative safeguards that health care organizations often struggle to implement and maintain – penalties for a violation are set at $50,000, and max out at $1.5 million annually. These technical and administrative safeguards include:

- **Access control:** All users must be given a unique username and password, and organizations must establish procedures that govern the access of ePHI as needed.
- **Authentication:** Electronic controls must be in place to verify that health information has not been illicitly altered or destroyed.
- **Encryption and decryption:** Messages sent beyond internal firewalls must be encrypted according to NIST standards, and decrypted when the message is received.
- **Activity audit controls:** Attempted access to ePHI must be logged, and any interaction with data during that access must be recorded.
- **Automatic logoff:** Once a certain amount of time elapses, authorized personnel must be automatically logged off unattended devices used to access or transmit ePHI.
- **Procedures for mobile devices:** This physical safeguard mandates the implementation of procedures to clear ePHI from lost or stolen devices (for instance, through the use of mobile device management tools).
- **Risk assessments:** Security officers must identify any areas where ePHI is in use and identify all ways in which that ePHI could be breached in a formal risk assessment.
- **Risk management policy:** Risk assessments are to be carried out regularly to identify and keep track of measures in place to manage risks.
- **Employee security training:** Formal, well-documented training sessions must review policies and procedures pertaining to ePHI, and the identification of malware.
- **Contingency plans:** A formal contingency plan must be created with the aim of facilitating uptime for critical processes and protecting ePHI during an incident.
- **Contingency plan testing:** Said plan must be tested periodically to assess the criticality of certain applications, and test backups of lost ePHI in an emergency event.
- **Restricting third-party access:** Unauthorized third parties (parent organizations, unauthorized vendors) must be barred from ePHI access.
- **Reporting security incidents:** There must be a framework to report security incidents (not necessarily breaches), and all employees should know how and when to report an incident, so as to take actions to prevent future breaches related to incidents.

Streamlining compliance management

Complying with HIPAA's technical and administrative rules requires complete visibility into all information systems. This calls for a security operation center staffed with dedicated security engineers capable of establishing baseline security configurations that comply with HIPAA, i.e., encryption standards, but also monitoring the network around the clock for noncompliant or suspicious behavior.

This SOC does not necessarily have to be operated in house – there are managed alternatives that are far more affordable but do the job just as proficiently. Nevertheless, it should exist in some capacity, both as a means for ensuring HIPAA compliance, and doing so in an efficient, streamlined manner.

ARCTIC WOLF

©2017 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com