HIC, Inc. Implementation, Enforcement, and Compliance Summary Plan (POL-SEC-007)

Daniel Cordeiro Marques

University of San Diego

CSOL-540-02-SP21 - Cyber Security Ops Policy

Professor Mike Hallman

April 18, 2021

Table of Contents

Introduction

As a health insurance company, HIC, INC. ("HIC") must follow applicable regulations such as the HIPAA Security Rule (Office for Civil Rights, 2013) and the HIPAA Privacy rule (Office of Civil Rights, 2003). HIC developed policies to safeguard sensitive data in alignment with these regulations and support the business needs. Therefore, failing to comply with such policies can lead to severe consequences to HIC, including regulatory fines and damage to HIC's reputation. The implementation, enforcement, and compliance plan establishes guiding principles to ensure that HIC appropriately implements and enforces controls and their compliance with the organizational policies.

Scope

The implementation, enforcement, and compliance plan applies to all employees and business associates responsible for and granted access to HIC information assets ("covered parties"). It also applies to HIC's information assets. These include systems and data supporting business functions (such as HR and finance) and assets processing, storing, and transmitting ePHI.

Objectives

Communications

General. HIC must provide the covered parties with information to implement and comply with the applicable policies, such as baseline checklists, policy documents, and training. HIC must ensure that this information is readily available through a website accessible to all covered parties. HIC must clearly communicate changes in policies and supporting documents

immediately after their approval. To comply with HIPAA requirements, HIC must maintain previous versions of policies and associated documents six years after their latest effective date (Office for Civil Rights, 2013). HIC must also establish communication channels between the covered parties and those responsible for maintaining the policy and supporting documents to clarify questions.

Onboarding communication. HIC must inform new covered parties of policies relevant to their roles before granting access to HIC's systems. Covered parties must also acknowledge they understand and will comply with the applicable policies.

Training

Onboarding training. HIC must train covered parties regarding policies and procedures relevant to their roles before granting access to HIC's systems.

Role changes. HIC must train covered parties regarding policies and procedures relevant to their new roles before promotions or changes become effective.

Training required by updates. HIC must train covered parties regarding updates in systems, policies, and procedures relevant to their roles.

Post-incident communication. After an incident occurs, HIC must contact covered parties to reinforce the policies associated with the event and provide lessons learned from the incident.

Annual training. HIC must provide yearly refreshment training for all users, covering applicable policies, updates, and lessons learned in the past year.

At the end of the training, the covered parties must also acknowledge they understand and comply with the applicable policies. HIC must maintain training records and covered parties' acknowledgments for at least six years after its completion.

Monitoring and Reporting

Continuous monitoring. HIC must deploy automated mechanisms to monitor compliance with the security and privacy policies, including scanning for unencrypted ePHI on servers and workstations, outdated endpoint protection software, and missed training. HIC must establish metrics to manage compliance against the organization's policies. The systems must report non-compliance to the appropriate supervisor and the Compliance Officer.

Threat and vulnerability monitoring. HIC must deploy automated mechanisms to identify vulnerabilities and indicators of attacks and unauthorized access to HIC information assets. These include network attacks, social engineering activity, and physical security breaches. Logs must be collected using a centralized server and cross-referenced. Events must be reported to the CISO and the Security Operations Center.

Reporting policy violations. Parties wishing to report policy violations should contact the Compliance Office to provide details regarding the event. The Compliance Office must make a reasonable effort to maintain violation reports anonymous.

Responsibilities

The CEO must approve the implementation, enforcement, and compliance plan.

The Chief Compliance Officer (CCO) is responsible for reviewing and approving the implementation, enforcement, and compliance plan. The CCO is also responsible for ensuring compliance with HIC policies and investigating compliance violations.

The CPO is responsible for ensuring the implementation, enforcement, and compliance plan aligns with relevant regulations and standards.

The CISO is responsible for reviewing and implementing threat and vulnerability monitoring.

The CTO is responsible for reviewing and implementing continuous monitoring of Information Technology assets.

Enforcement and Exceptions

The CEO, CCO, and CPO must formally approve exceptions to the privacy policy. HIC will apply sanctions to any parties failing to comply with their responsibilities.

Review and Revision

The CCO and CPO must review this policy annually or in case of significant changes in the business requirements and threat landscape. The CCO and CEO must approve any recommended changes.

References

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (Special Publication 800-53, rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Office for Civil Rights. (2013, July 26). Summary of the HIPAA Security Rule. U. S. Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Office of Civil Rights. (2003). Summary of the HIPAA Privacy Rule. U. S. Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html