HIC, Inc. Asset and Information Classification Policy (CONFIDENTIAL - POL-SEC-003)

Daniel Cordeiro Marques

University of San Diego

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

Professor Mike Hallman

April 5, 2021

Table of Contents

Introduction

HIPPA's Privacy Rule requires that covered entities classify and group data according to their sensitivity levels (Office for Civil Rights, 2003). This asset and information classification policy outlines the classification scheme and the requirements to safeguard assets and information according to their classification. The classification layers are based on the "Legal Classification Scheme" proposed by Johnson (2014). This model allows users to quickly understand the information classification while enabling Information Security to apply appropriate measures to safeguard information effectively and cost-efficiently according to the risks affecting data handled by HCI's systems and users.

Scope

This asset and information classification policy is mandatory. It applies to all employees and business associates granted access to HIC information assets ("covered parties"), including systems and data supporting business functions (such as HR and finance) and assets processing, storing, and transmitting ePHI.

Objectives

Asset and Data Classification

Restricted. Assets and data must be classified as "restricted" if events impacting their confidentiality, integrity, or availability result in severe damage to HIC, including regulatory fines. Protected health information (PHI), Personally Identifiable Information (PII), and systems that handle them must always be classified as restricted.

Confidential. Assets and data must be classified as "confidential" if events impacting their confidentiality, integrity, or availability result in significant damage to HIC, including reduced competitive advantage. Examples include financial statements before their presentation to the board of directors and internal documents. This policy is classified as public.

Public. Assets and data must be classified as “public” if events impact their confidentiality, integrity, or availability result in little or no damage to HIC. Users may distribute public information widely, such as campaigns approved by the marketing department at the release date.

Authorized Use

Upon creation, users must label data and assets as “Restricted,” “Confidential,” and “Public” according to this policy. Users must not copy information between assets in different layers. For instance, a user must not move data from a restricted asset to a confidential one unless formally approved by the data owner. Users are not allowed to access data and assets labeled as “Restricted” unless required to perform their job functions. The data owner will grant and document access upon review and authorization of a formal request. Specifically:

Classification	Authorized users	User responsibilities
Restricted	Access to these assets and data is allowed on a need-to-know basis according to the user’s role, such as billing information to claims personnel.	Users must store, transmit, and destroy restricted information using restricted assets. Users must only share restricted information with authorized users.
Confidential	Only internal personnel and authorized business partners can access confidential information assets.	Users must store, transmit, and destroy restricted information using confidential assets. Users must only share confidential information with authorized users.
Public	General public	Users must store, transmit, and destroy restricted information securely

Responsibilities

The CEO must approve the asset and information classification policy.

The CIO is responsible for reviewing and approving the asset and information classification policy.

The CISO is responsible for enforcing access control according to the asset and information classification policy.

The CPO is responsible for ensuring the asset and information classification policy compliance with applicable laws.

Data Owners (department leads) are responsible for ensuring the appropriate classification of assets and information according to this policy.

Data Users are responsible for labeling and using the HIC assets and information following this policy.

Enforcement and Exceptions

HIC must train users to identify their roles use and classify assets accordingly. The CISO, CPO, and data owners must formally approve exceptions to this policy. HCI will apply sanctions to any parties failing to comply with their responsibilities. An automated tool must proactively monitor policy deviations and perform weekly scans to identify restricted and confidential information inappropriately stored and transmitted.

Review and Revision

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

References

Johnson, R. (2014). *Security Policies and Implementation Issues* (2nd ed., Kindle ed.). Jones & Bartlett Learning.

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