HIC, Inc. Privacy Policy (POL-SEC-004) Summary

Daniel Cordeiro Marques

University of San Diego

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

Professor Mike Hallman

April 12, 2021

Table of Contents

Introduction

HIC, INC. ("HIC") collects, stores, and processes private information from clients and business associates to achieve its business objectives. As patient and partner privacy is the cornerstone of HIC's operations, the organization must develop safeguards to protect sensitive data and comply with the applicable regulation. This privacy policy summary delineates HIC's privacy domains, relevant laws and standards, and the responsibilities of revoking and granting access to information.

Scope

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

Objectives

Public Company Information Domain

Data covered by the Public Company Information Domain. This domain covers information HIC shares with the public and does not contain private data from business associates or patients. It includes public marketing materials public financial information such as quarterly and annual reports, job postings, and press releases.

Applicable law and standards. As a healthcare provider, HIC is covered by HIPAA. The HIPAA Privacy Rule (Office of Civil Rights, 2003) establishes requirements to safeguard ePHI; COPPA (Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505, 1998) makes provisions to protect sensitive information for children under 13 years old.

Data privacy responsibilities. The Chief Financial Officer (CFO) must approve the issuance of financial-related data. The head of Marketing must authorize the publication of information associated with HIC's brand (such as marketing materials and press releases). Department heads must allow the public dissemination of information. For instance, the head of HR must approve the advertising of Job postings. To ensure compliance with applicable privacy law, the Chief Privacy Officer is responsible for reviewing the information before publication.

Private Patient information Domain

Data covered by the Private Patient Information Domain. This domain covers electronic protected health information (e-PHI) and patients' billing information. HIC and business partners can only use this information for medical purposes and provide insurance services. Private Patient Information should never be available to the public.

Applicable law. HIPAA (as it covers both ePHI and billing information), COPPA, and PCI DSS. The PCI DSS makes provisions regarding payment system security, and HIC should follow it to protect systems handling billing for patients.

Data privacy responsibilities. The medical department heads, such as the head of oncology and general practice, are responsible for granting and revoking patient data access. The director of billing services is responsible for authorizing access to billing information.

Private Employee Information Domain

Data covered by the Private Employee Information Domain. This domain encompasses employees' personally identifiable information (PII), including payroll information, name, address, and social security numbers.

Applicable law. The Electronic Communications Privacy Act of 1986 (ECPA) protects "protects wire, oral, and electronic communications," including employee communications over email and telephone (Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2523, 1986). Since HIC operates only in Texas, no state privacy laws affect HIC's operations.

Data privacy responsibilities. The HR director and the CPO are responsible for granting and revoking access to information in this domain.

Restricted Corporate Information Domain

Data covered by the Restricted Corporate Information domain. This domain covers the information restricted to HIC's internal use, such as financial statements, intellectual property, and confidential policies.

Applicable laws and standards. The PCI DSS applies to this domain, as it makes provisions on segmentation between systems handling payment data and other assets. The HIPAA Security Rule (Office for Civil Rights, 2013) also calls for safeguards that separate ePHI from non-covered information.

Data privacy responsibilities. The CIO and the CISO are responsible for granting and revoking access to information in the Restricted Corporate Information domain.

Responsibilities

In addition to those outlined in each domain, this section covers additional responsibilities.

The CEO must approve the privacy policy.

The CIO is responsible for reviewing and approving privacy policies.

The CISO is responsible for reviewing and enforcing access control according to the privacy domains and policy.

The CPO is responsible for ensuring the privacy policy aligns with relevant regulations and standards.

Enforcement and Exceptions

HIC must give clear and adequate notice to employees, patients, and business partners regarding data collection, use, and storage. The organization must provide annual training and make the privacy policy readily available on the website. The CISO 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 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

Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. (1998). *https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule*

Electronic Communications Privacy Act of 1986 (ECPA) & 18 U.S.C. §§ 2510-2523. (1986). *https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285*

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*