CSOL540 Module 5: Information Classification Scheme

John C. McGovern

University of San Diego

April 3rd, 2021

Introduction

The Health Insurance Company (HIC) is fundamentally an information company. HIC ingests, processes, analyses, and actions on large amounts of data related to customer health and coverage for medical claims. A breach in the confidentiality of customer data would have severe ramifications to the organization, including loss of customer trust, loss of revenue, and even the potential failure of the organization as a whole (Zorabedian, 2020).

This document outlines the four HIC information classification levels presented in order from least to most confidential. These classifications are to be understood by all employees. Furthermore, they are to be used in defining the security classification and tagging of documents, systems, and applications to ensure the appropriate handling of information.

Public

The HIC public information classification is the definitionally least restrictive classification within the four-tier system. However, the Public classification is actually comparatively less common given the nature of the HIC business. Public information has been reviewed by marketing, legal, and compliance teams and has been deemed as allowable for public posting. This tier of data is more commonly used in the HIC Marketing and Public Relations organizations but less so in other organizational units.

Public data has been fully vetted and cleared for public release and is allowed to be posted publicly in press releases, marketing materials, public websites, and other public outlets. However, it is important to consider that Public data is rarely automatically public and must be reviewed and classified as such through the companies Approved Public Information Release (APIR) process. Employees must be aware of this review phase and never assume data is public until approved. Once data has been given a "Public" label, any employee, as well as customers and external constituents, can view the information without restriction.

Internal

Information that receives the "Internal" label is the most common type of non-customer corporate data. Employees performing their normal duties and are most commonly generating or viewing Internal data. Examples include most employee-to-employee communications such as e-mails, voice messages, Slack messages, and internal documentation. Most internal business-to-employee communications are also considered Internal data. All employees are allowed to read and create Internal data, and most will do so in the course of employment with HIC. Some Internal information is restricted to departments for their specific use. In this case, the relevant information is labeled as "Internal (Department Name)" such as "Internal (Marketing)."

Internal information is not intended for public consumption unless it undergoes the APIR process and is fully relabeled. Generally, no special clearance is required to view such data, but corporate privacy policies do apply. For example, an employee should not read another employee's e-mail without approval and human resources authorization. Breach of HIC Internal information is serious and can result in an action against the employee for mishandling data.

Confidential

Confidential information is a somewhat less common label within HIC but is critically important to the organization's operation. Confidential data is the highest classification given to data that does not contain customer information (restricted information). Confidential data is information that is of strategic business value to the organization and must be protected at all costs. This includes information such as employee personal information, HR and legal communications, financial and earnings data, and proprietary records specific to the company's operation. This classification includes material non-public information as defined by the Securities and Exchange Commission (SEC) until that data is released publicly as part of corporate filings (Chen, 2020).

Confidential information may also be restricted to a department's access using the same convention mentioned above (i.e., Confidential (Human Resources)). Employee access to confidential data is heavily restricted by role, and confidential data is rarely released to the public except for in the case of required disclosures and financials as described above. Employees responsible for creating and handling confidential data must take additional information security training yearly, and responsibility for a breach is a likely cause of termination.

Restricted/Protected

Restricted information (also known as Protected Health Information) is the most sensitive data HIC handles (Adler, 2018). The primary differentiator for Restricted classification is if the data contains any customer information such as (but not limited to) name, location, demographic, identification number(s), health status, procedure information, provider information, or claim status. Any loss of Restricted data can result in a breach disclosure notification, fees for restitution, fines, and other losses to the corporation (Alder, 2021). As such, an employee that is responsible for such a data breach may be subject to termination. Given the nature of HIC's business, many employees require access to role-appropriate restricted records. This makes protecting this information each employee's responsibility. Training is provided on data classification with a specific emphasis on Restricted information.

Conclusion

Understanding HIC information classification and handling information appropriately is every employee's responsibility. Training on information classification is provided at least yearly depending on employee role. Inappropriate disclosure can result in loss of customer trust, significant revenue impact, and, in some cases, consequences to the individual or group responsible.

References

Alder, S. (2018, January 10). *What is Protected Health Information?* HIPAA Journal. https://www.hipaajournal.com/what-is-protected-health-information/

Alder, S. (2021, January 15). *What are the Penalties for HIPAA Violations?* HIPAA Journal. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

Chen, J. (2020, November 19). *Material Nonpublic Information Definition*. Investopedia. https://www.investopedia.com/terms/m/materialinsiderinformation.asp

Zorabedian, J. (2020, August 13). *What's New in the 2020 Cost of a Data Breach Report*. Security Intelligence. https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/