Data Classification at HealthCare Solutions Inc.

By
Angel
Contreras

Dr. Arun Aryal CIS
4880 February 20,
2025

TABLE OF CONTENTS

Introduction

Company Background

Data Categorization

Data Classification Standards

- Types of Data & Their Classification – Private Data
- Types of Data & Their Classifications – Confidential
- Types of Data & Their Classifications – Internal Use Only
- Types of Data & Their Classifications – Public Domain Data

Purpose of Data Classification Standards

Data Security Recommendation and HIPPA Requirements

Conclusion

Refrences

COMPANY BACKGROUND

CareAtHome is certified by the California Department of Social Services' Home Care Services Bureau. A small home healthcare business that provides nursing and therapy services to patients in their homes. CareAtHome handles sensitive patient data, including medical records, billing information and personal details. However, the company lacks a formal data classification system, which has led to inconsistent data handling practices and increase risks of data breaches.

CAREATHOME

YOUR HOMETOWN HOME CARE

DATA TYPES

Patient Medical Records: Personal health information, treatment histories, prescriptions, lab results.

Billing Information: Invoices, payment records, insurance details.

Employee Records: Personal details, employment history, payroll information.

Internal Communications: Emails, meeting notes, internal memos.

Data Type	Sensitivity	Importance
Patient Medical Records	Very High	Crucial
Billing Information	High	Important
Employee Records	Medium	Moderate
Internal Communications	Low to Medium	Varies

Classification System

Public
Definition: Data that is freely available to the public.
Examples: Company press releases, marketing materials, published articles.

Internal
Definition: Data meant for internal use within the organization.
Examples: Internal communications, employee manuals, internal reports.

Private
Definition: Sensitive data that requires restricted access to authorized personnel.
Examples: Employee records, internal financial data, business strategies.

Confidential
Definition: Highly sensitive data that requires strict access control and protection.
Examples: Patient medical records, billing information, proprietary information.

Data Classification Policy

Purpose: The purpose of this policy is to establish a framework for classifying and handling data based on its sensitivity and importance to CareAtHome.

Scope: This policy applies to all employees, contractors, and third parties who have access to CareAtHome's data.

Guidelines:

- Criteria for Classifying Data:
- Data should be classified based on its content, legal requirements, and potential impact on the organization.
- Data owners are responsible for determining the appropriate classification level.

Roles and Responsibilities:

- Data Owners: Responsible for classifying data and ensuring its protection.
- Employees: Responsible for handling data according to its classification.
- IT Department: Responsible for implementing and maintaining security measures.

Procedures for Handling and Storing Data:

- Public Data: May be freely distributed and stored with minimal security.
- Internal Data: Should be accessed only by employees and stored in secure systems.
- Private Data: Requires access controls and encryption during transmission and storage.
- Confidential Data: Requires strict access controls, encryption, and regular audits.

Recommended Security Measures

Public:

- No special security measures required, but ensure data integrity.

Internal:

- Access controls (role-based access).
- Regular employee training on data handling.

Private:

- Strong access controls (multi-factor authentication).
- Encryption during transmission and storage.
- Regular security audits.

Confidential:

- Strict access controls (need-to-know basis).
- Advanced encryption methods.
- Continuous monitoring and logging.
- Regular compliance audits.

Alignment with HIPPA Requirements

Ensure all electronic protected health information (ePHI) is encrypted.

Implement access controls to limit data access to authorized personnel only.

Conduct regular training and awareness programs for employees on HIPAA compliance.

Regularly audit and monitor systems to detect and respond to potential security incidents.

CONCLUSION

Data classification and policy development are crucial for protecting CareAtHome's sensitive information. By categorizing data into Public, Internal, Private, and Confidential levels, CareAtHome can apply appropriate security measures and comply with HIPAA requirements.

The Data Classification Policy provides clear guidelines for classifying and handling data, assigning roles and responsibilities, and implementing security measures for each classification level. This comprehensive approach ensures that patient, billing, employee, and internal data are protected, fostering a culture of security and trust within the organization.

By adopting these practices, CareAtHome can maintain high-quality care while safeguarding the privacy of its patients and stakeholders

References

Care at Home - Care At Home. (2024, June 3). Care at Home. https://careathomellc.com

U.S. Department of Health and Human Services. (2022, October 19). *Summary of the HIPAA privacy rule*. HHS.gov; U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Thank You!