Enhancing Data Governance and Security: A Strategic Plan for MaineHealth

Position Paper 1, DSE6003

Adeline Casali

September 7, 2023

# Introduction

## Key Governance, Security, and Ethical Issues

The healthcare industry is one of the most susceptible to security attacks, as the data from healthcare companies is typically private and confidential. This sensitive information is highly valuable to hackers, making the industry a large target for attacks (Seh et al., 2020). This vulnerability is particularly pertinent in the era of big data, as the current trend towards digitizing healthcare has led to an enormous quantity of clinical data availability. Although big data holds the promise of opportunities and the potential to lower costs, improve care, and even save lives, it also introduces a host of data security issues due to the quantity and complexity of the data (Abouelmehdi et al., 2017).

A data breach is defined as “a security incident in which sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorized individual” (Khan et al., 2021, p. 2). Data breaches are surprisingly common in the healthcare industry. Between 2005 and 2019, 249.09 million individuals worldwide were impacted by healthcare data breaches (*Data Breach Chronology*, 2023). And in 2022 alone, 51.9 million healthcare records were exposed, stolen, or illegally disclosed (Alder, 2023). Furthermore, these breaches can be extremely costly to the organization. According to IBM’s 2023 Cost of a Data Breach report, the average healthcare data breach in 2022 in the United States cost $10.93 million (IBM, 2023). Avoiding data breaches is one of the leading security goals of this plan.

# Data Governance Framework

## Data Governance Policies

As an overview, data governance involves the utilization of oversight, authority, and control in managing data. Its primary objective is to enhance the worth of data while reducing the expenses and potential risks associated with it (Abraham et al., 2019). Protocols must be put into place the clearly define roles, responsibilities, and accountability for data stewardship, quality, and compliance. These policies should align with industry best practices as well as legal regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) (Kaplan et al., 2023).

## Data Governance Committee

We will establish a Data Governance Committee consisting of key stakeholders from IT, legal, compliance, and business units. This committee with oversee all data-related policies and decisions, as well as be available as a data breach response team in the case of a data security incident.

## Data Inventory and Classification

Data will be inventoried and classified based on sensitivity and confidentiality.

## Data Privacy and Ethics

Data anonymization, k-anonymity, see Sweeney 2002 for an example. Include a description of differential privacy – reference paper from class.

# Data Security Measures and Protocols

## Data Security Framework

## Data Backup and Recovery

Mention cloud storage issues!

## Incident Response Plan

# Data Access, Usage, and Sharing Mechanisms

## Access Controls

## Data Usage Policies

An Acceptable Data Use policy will be defined and implemented, which states

## Secure Data Sharing

## Employee Training

Training will be provided to new employees within the first week of starting the position and current employees on a yearly basis. This training will cover the company’s Acceptable Use Policy (AUP) as well as other privacy rules such as HIPAA, and how to report a data breach. This training will be interactive and include discussion, to ensure that employees are engaged and understand objectives and policies (National Forum on Education Statistics, 2020).

# Conclusion

References: