# Access Management and Data Security Plan
# Victor Onukwu
# W10D2

# Table of Content

# Executive Summary

This document outlines the access management and data security plan for a hypothetical healthcare organization, HealthCareX.

The plan includes role-based:

Access control by roles;

- Doctor
- Nurses
- Billing Department

Data security measures;

- Encryption
- Regular Audit
- Two-Factor Authentication

Response plan for potential data breaches;

- Identify and Contain
- Investigate and Report
- Notify and Mitigate

By implementing role-based access control, robust data security measures, and having a clear response plan, HealthCareX can ensure the security and privacy of its patient data

# Introduction

HealthCareX is a healthcare organization that handles sensitive patient data, including personal identification information(PII), medical histories, and insurance details. Ensuring the security of this data is paramount to maintain trust and comply with regulations such as Health Insurance Portability and Accountability Act(HIPAA).

# Access Management

Three main roles within HealthCareX require access to data:

1. **Doctors:** Doctors need access to comprehensive patient data, including medical histories, current medications, and test results, to provide appropriate care.
2. **Nurses:** Nurses require access to a subset of patient data, including current medications and basic patient information, to administer care.
3. **Billing Department:** The billing department requires access to insurance details and services provided, but not to specific medical data.

# Data Security Measures

HealthCareX should implement the following data security measures:

1. **Encryption:** All data, both at rest and in transit, should be encrypted to prevent unauthorized access even if there is a breach.
2. **Regular Audits:** Regular audits of access logs can help detect any unauthorized access attempts or anomalies.
3. **Two-Factor Authentication (2FA):** 2FA provides an additional layer of security, ensuring that users must verify their identity through a second method besides just a password.

# Response Plan

In case of a data breach, HealthCareX should follow these steps:

### Identify and Contain (Preparation and Prevention)

This stage involves identifying the source of the breach and containing it to prevent further data leakage. In the NIST framework, this falls under the preparation and prevention stage. It involves having measures in place to quickly identify potential threats and contain them. This could involve isolating affected systems or blocking malicious IP addresses.

### Investigate and Report (Detection and Analysis)

Once the breach has been contained, a thorough investigation is conducted to understand the extent of the breach. This aligns with the detection and analysis stage of the NIST framework. The aim is to understand the nature of the incident, the systems or data affected, and the potential impact. The findings of this investigation are then reported to the necessary regulatory bodies, in compliance with legal and contractual obligations.

### Notify and Mitigate (Containment, Eradication, and Recovery)

After the investigation, affected individuals are notified. This falls under the containment, eradication, and recovery stage of the NIST framework. The organization takes steps to mitigate the effects of the breach, such as offering credit monitoring services. The organization also works to eradicate the threat from their systems and recover any affected services or data.

# Conclusion

By implementing role-based access control, robust data security measures, and having a clear response plan, HealthCareX can ensure the security and privacy of its patient data. Regular reviews and updates of these plans are necessary to adapt to evolving threats and technologies.

# References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

CrowdStrike. (n.d.). Incident response steps: A guide to handling breaches. https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

Bing. (n.d.). Retrieved November 23, 2023, from https://bing.com/search

Cynet. (2020, October 14). NIST Incident Response: A Guide to the NIST Cybersecurity Framework. Cynet. https://www.cynet.com/incident-response/nist-incident-response/