Table of Contents

[Introduction: 1](#_Toc144196801)

[Applicable Security Standards: 1](#_Toc144196802)

[General Data Protection Regulation (GDPR): 1](#_Toc144196803)

[Payment Card Industry Data Security Standard (PCI DSS): 1](#_Toc144196804)

[Health Insurance Portability and Accountability Act (HIPAA): 1](#_Toc144196805)

[Evaluation of Compliance: 1](#_Toc144196806)

[Reviewing Data Handling Practices: 1](#_Toc144196807)

[Security Infrastructure Inspection: 1](#_Toc144196808)

[PHI Protection Assessment: 1](#_Toc144196809)

[Recommendations for Meeting Standards: 2](#_Toc144196810)

[GDPR Compliance Recommendations: 2](#_Toc144196811)

[PCI DSS Compliance Recommendations: 2](#_Toc144196812)

[HIPAA Compliance Recommendations: 2](#_Toc144196813)

[Assumptions Made: 2](#_Toc144196814)

[References: 2](#_Toc144196815)

Security Standards Assessment

# Introduction:

In this E-Portfolio exercise, we will analyse the security standards applicable to a given organisation, evaluate its compliance, and provide recommendations based on the provided sources. The organisation under consideration will be subject to the following security standards: General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and the Health Insurance Portability and Accountability Act (HIPAA).

# Applicable Security Standards:

General Data Protection Regulation (GDPR):

This standard would apply to any organisation that processes personal data of individuals in the European Union (EU). It ensures the protection of personal data and the privacy rights of EU citizens (ICO, 2020).

Payment Card Industry Data Security Standard (PCI DSS):

Organisations that handle online payments or credit card transactions must adhere to PCI DSS. This standard ensures the security of cardholder data to prevent breaches and fraud (PCI Security Standards.org, 2020).

Health Insurance Portability and Accountability Act (HIPAA): Healthcare organizations in the United States that handle protected health information (PHI) must comply with HIPAA. It safeguards the confidentiality and security of patients' sensitive medical information (HIPAA, 2020).

# Evaluation of Compliance:

To check if the organisation is meeting these standards, a comprehensive assessment would be necessary. This could involve:

Reviewing Data Handling Practices:

For GDPR compliance, the organisation's data processing practices should be audited to ensure proper consent mechanisms, data minimisation, and data subject rights management.

Security Infrastructure Inspection:

For PCI DSS compliance, the organisation's payment processing systems and security controls should be reviewed to ensure cardholder data protection and secure transmission.

PHI Protection Assessment: For HIPAA compliance, a thorough evaluation of the organisation's handling of protected health information would be necessary, including access controls, encryption, and incident response procedures.

# Recommendations for Meeting Standards:

## GDPR Compliance Recommendations:

* Implement a clear and accessible privacy policy.
* Establish a data protection officer responsible for GDPR compliance.
* Conduct regular data protection impact assessments.
* Obtain explicit consent for data processing activities.

## PCI DSS Compliance Recommendations:

* Use secure encryption for cardholder data transmission.
* Implement strong access controls to limit cardholder data access.
* Regularly test and update security systems and processes.
* Segment networks to isolate cardholder data environment.

## HIPAA Compliance Recommendations:

* Encrypt electronic PHI to ensure data confidentiality.
* Implement strict access controls and audit logs for PHI.
* Develop and test an incident response plan for data breaches.
* Train staff on HIPAA regulations and security practices.

# Assumptions Made:

* The organisation processes personal data of EU citizens, requiring GDPR compliance.
* The organisation handles online payments, necessitating PCI DSS compliance.
* The organisation deals with protected health information, mandating HIPAA compliance.

# References:

1. ICO. (2020) Guide to the General Data Protection Regulation (GDPR).
2. PCI Security Standards.org. (2020) Official PCI Security Standards Council Site - PCI Security Standards Overview.
3. HIPAA. (2020) HIPAA For Dummies – HIPAA Guide.