Seminar 4 Preparation: Security Standards

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: N/A

Date: Friday 1st October 2021

Student ID: 126853

Which of the standards discussed in the sources above would apply to the website/ organisation assigned to you for the assessment?

Out of the 3 standards discussed in the Seminar webpage (GDPR, PCI-DSS, HIPAA), only the GDPR legislation would apply to the e-Health site assigned to us for the Unit 6 and 11 assessments. The Health Insurance Portability and Accountability Act (HIPAA) applies only to companies operating within the US, whereas GDPR applies to any organisation processing data on a European citizen.

Evaluate your assigned website against the appropriate standards and decide how you would check if standards were being met?

In its current state, I would consider the e-Health site we have been assigned to be non-compliant with the provisions of GDPR. As the website processes Personally Identifiable Information (PII), it is required to gain consent from the user at the point of creating a post, as well as displaying a public Privacy Notice, informing users of what information is collected, for which purpose and who is responsible for the information.

In order to check whether the standards are being met, a business would need to audit all of its data collection/processing functionalities – ensuring they have a lawful basis for processing the data, as well as provide the functionalities available to data subjects (Subject Access Request, Subject Erasure Request etc.)

What would your recommendations be to meet those standards?

In order to meet the GDPR standards, I would recommend that the e-Health provider takes the following actions:

- Undertakes a full audit of data collection/processing functionalities. They should establish the lawful basis for processing and collection of all data, as well as ensure they are completely transparent with their users.
- Implements a data retention policy, ensuring that non-essential data is deleted or anonymised after a specific period of time.
- Ensures that information is stored in a secure manner (Encryption) and is only accessible to the users that need it (Medical Practitioners, the end-user etc.)

What assumptions have you made?

When creating this document, I have made the following assumptions:

- The E-Health provider is based within the United Kingdom (UK).
- The entirety of the E-Health site is currently available.