**Security Awareness Training**

You are the Cybersecurity lead for a large hospital in Texas. A recent audit has found that the security awareness training program is woefully deficient. As you might expect, the hospital is subject to HIPAA (​Health Insurance Portability and Accountability Act) requirements. The specific HIPAA Rule is ​§164.308.(a).(5).(i) – Implement a security awareness and training program for all members of its workforce (including management).

In addition, Texas’s Health Privacy Law, ​H.B. No. 300 § 181.101,​ requires employees to be trained about both the state’s law and HIPAA.​ ​Texas is one of the few states that mandates training about Texas’s own health privacy law. Additionally, it requires training about HIPAA. Penalties for violating the Texas law are quite high, equivalent to HIPAA.

You have been asked to address this audit finding by completely throwing out the old training and starting over. ​**To this end, you have been asked to supply the following**:**​**

1. A security awareness program framework, an explanation of why it is needed, and the potential cost in terms of noncompliance. Note: the cost of not complying is not always limited to fines and penalties!

* Objectives and goals for the program
* The program's scope which employees it will cover
* Training delivery method such as in-person, online, or hybrid
* Training frequency like annually, biannually, or as necessary
* Mechanisms for monitoring and reporting training completion and comprehension among employees
* Regular evaluations of the program's performance.

* To make sure that every employee is aware of the value of protecting sensitive information and how to do so, a security awareness program is required. This includes confidential information about the hospital as well as health and personal information about the patients. Human error, which is the main reason for data breaches in healthcare institutions, is prevented by the application. Risks associated with noncompliance, fines, legal fees, and reputational harm to the hospital may be imposed as a result of failure to abide by HIPAA and the Texas Health Privacy Law. A leak of patient information may also damage the hospital's reputation and cause patients to lose faith in it. Noncompliance can also result in a decline in sales since patients may choose a hospital that has a better history of keeping its information secure.

1. Specific items that need to be addressed in the training per HIPAA and/or Texas statutory requirements.

* An overview of the Texas Health Privacy Law and HIPAA, including the responsibilities of employees and the consequences of noncompliance
* Knowledge of the characteristics of sensitive information, such as patient health information, personal information, and private hospital information.
* The Significance of safeguarding private information and the repercussions of a breach
* How to handle and get rid of sensitive information like encryption, password protection
* Recognizing and disclosing alleged security breaches and occurrences
* How to identify and stay away from social engineering and other forms of phishing attempts.
* Guidelines for safely using medical technology and equipment
* The importance of ongoing education and remaining current with dangers and laws that are changing.
* Phishing attacks
* Removable media
* Passwords and Authentication
* Physical security
* Mobile Device Security
* Working Remotely
* Public Wi-Fi
* Cloud Security
* Social Media Use
* Internet and Email Use
* Social Engineering
* Security at Home

1. List of internal groups or departments that should be consulted before the awareness training is submitted to management for final approval.

* Human resource
* Legal
* Marketing
* physical security