COSC 4361
A Comprehensive Legal and Ethical Framework Analysis, Security Policy Development, Incident Response Plan, and Business Impact Analysis for The University of Texas Health Science Center

By: Sandhya Malla

Introduction to UTHSC

UTHealth

The University of Texas
Health Science Center at Tyler

Basic Legal and Ethical Framework Analysis

HIPAA

HIPAA and InfoSec

Complying with HIPAA and the Consequences for Non-Compliance

HIPAA

- Federal law established in 1996
- Enhances portability of health insurance
- Protects the privacy of patients and health plan members
- Ensures security of health information
- Mandates notification of breaches concerning health data

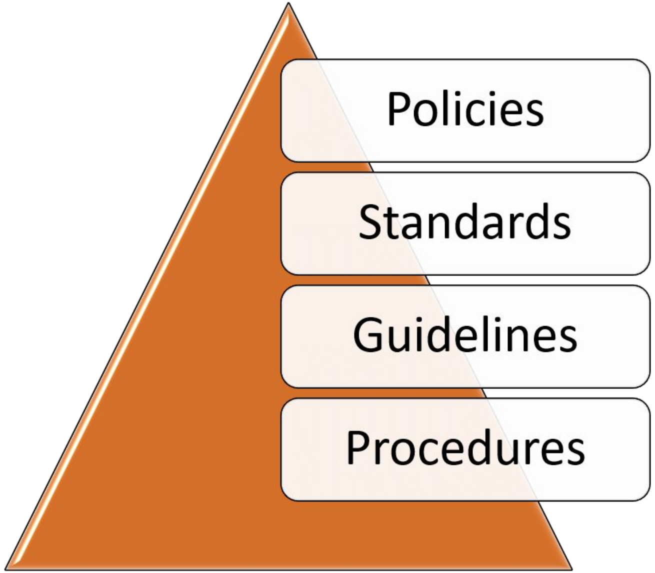
HIPAA and InfoSec

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit.
- Identify and protect against reasonably anticipated threats to the security or integrity of the information.
- Protect against reasonably anticipated, impermissible uses or disclosures.
- Ensure compliance by their workforce.

Compliance

- Strong access control to prevent unauthorized access.
- Ensuring confidentiality, integrity, and availability of records.
- Intrusion detection and prevention system with a detailed threat database.
- Ensuring workforce compliance.

Policy Framework



Policies

Standards

Guidelines

Procedures

ISSP 1: Device/Data Retention

- Authorized Uses
- Prohibited Uses
- Systems Management
- Violations of Policy
- Policy Review and Modification

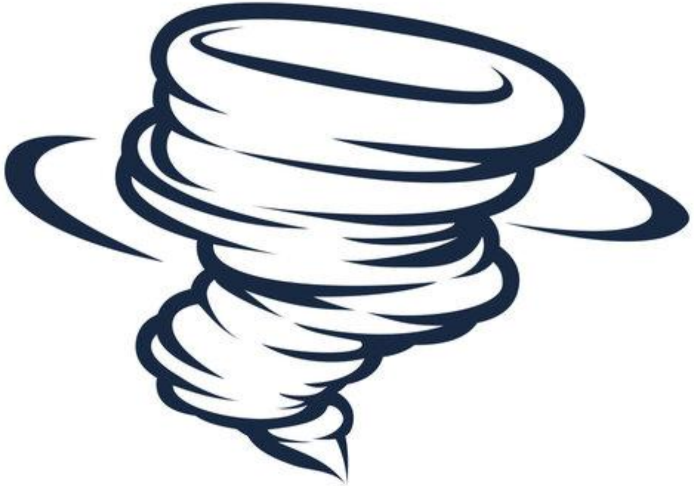
ISSP 2: Personal Devices on UTHSC’s Network

- Authorized Uses
- Prohibited Uses
- Systems Management
- Violations of Policy
- Policy Review and Modifications
- Limitations of Liability

Business Impact Analysis and Incident Response Plan

Natural Disaster: Tornado

- Business Impact Analysis
  - Patient care may be interrupted
  - Data loss, lab disruptions
  - Damage to hardware infrastructure
  - Disruption of administrative functions
- Incident Response Plan
  - Communication Plan
  - Response Strategies
  - Recovery Strategies



Man-Made Incident: Ransomware

- Business Impact Analysis
  - Patient Care (Records; PII, e-PHI, Hospital operations)
  - Research Activities (Data Loss)
  - Disruption of Administrative Functions
  - Disruption of business operations
  - Corruption of databases
- Incident Response Plan
  - Communication Plan
  - Response Strategies
  - Recovery Strategies

Conclusion