CSC 116 Introduction of Cybersecurity

**Assignment 2**

**Notes**:
1 Write your answers in a new word document including your team number and members, and share it with our TA Caden before **02/22/2025.**
email: crh873@miami.edu.
2 No ChatGPT or any other generative AI (e.g., Calude or Copilot) are allowed for answering all the assignments. **Generative AI is only eligible for grammar editing and sentence improvements.**

**1. Message Authentication in Healthcare**

Why is it important to ensure that electronic health records (EHRs) or prescriptions sent between healthcare providers are protected by a Message Authentication Code (MAC)? Explain how HMAC prevents tampering during transmission.

*Hint: Message Authentication Code is for ensuring data authenticity.*

**2. Role-Based Access Control (RBAC)**

A hospital uses RBAC to limit access to patient records. Nurses can only view records of patients they are assigned to, while doctors can edit records. Explain why RBAC is critical in healthcare and how it improves patient privacy.

**3. Digital Signatures for E-Prescriptions**

Digital signatures are used to sign e-prescriptions. Describe how digital signatures ensure authenticity, integrity, and non-repudiation. Why is this important for preventing prescription fraud?

**4. Principle of Least Privilege**

As a nurse, you need access to patient records to update vital signs. Why should your access permissions not include deleting patient records? Relate your answer to the Principle of Least Privilege.

**5. Data Backup and Recovery**

A ransomware attack encrypts a hospital's patient database. Explain why regular backups are essential in this scenario. What types of backup storage (local, off-site, cloud) would you recommend, and why?

**6. Authentication Methods in Healthcare**

Compare knowledge-based authentication (e.g., passwords) and biometric authentication (e.g., fingerprint scans) in a hospital setting. Which method is more secure for accessing sensitive patient data? Justify your answer.

**7. Access Control**

A hospital policy states: "Doctors can access patient records only during their shifts and from hospital devices." Which access control model (ABAC, RBAC, MAC) enforces this rule? Explain how this protects patient data.

**8. Hash Functions for Data Integrity**

Explain how a hash function like SHA-256 ensures the integrity of a patient's lab report. What happens if a single character in the report is altered accidentally?

**9. Certificates and Secure Communication**

Why do healthcare portals use digital certificates? How do certificates prevent attackers from impersonating a hospital's website to steal patient credentials?

**10. Non-Repudiation in Consent Forms**

A patient signs a digital consent form for surgery. How does non-repudiation ensure the patient cannot later deny signing the form? What role do public/private keys play in this process?
*Hint: Digital signature.*