CSC 116 Introduction of Cybersecurity

Assignment 5

Notes:
1 Write your answers in a new word document including your team number and members, and share it with our TA Caden before **04/15/2025.**
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. Data Anonymization
Question:

Hospitals often need to share patient data for research but must protect patient identities (e.g., name, zip, address, sex, etc.). In your own words, explain what **data anonymization** means. Give one example of how this technique could help nurses protect patient privacy in daily work.

Hints: Explain what is data anonymization and how to use it to protect patient data.

2. Secure Multi-Party Computation / Differential Privacy / Threshold Signatures
Question:

Several hospitals want to train an AI model to predict diseases, but none of them want to share patient data directly. In your own words, describe what you understand about **secure multi-party computation** or **differential privacy**. How could this allow hospitals to work together without risking patient privacy?

Hints: Federated learning for training global AI models. Using differential privacy to protect the gradient descent.

Open question: Discuss how threshold signatures can be used here.

3. Homomorphic Encryption
Question:

A hospital wants to use a cloud AI service to analyze CT scans, but they are worried about sending sensitive data over the internet. **Homomorphic encryption** allows AI to work on encrypted data without ever seeing the raw image. Explain this idea in your own words and discuss how it could protect patient privacy in medical imaging.

Hint: please also discuss the limitation of HE as we discussed HE has a lot of drawbacks.