# DSCI 519 Semester Project

## Nature of the assignment

The semester project gives each student the opportunity to use and illustrate concepts from the course in an applied, “real world” manner. You are asked to review a human language law, extract the information security and privacy-relevant portions, and summarize them. In addition, you must consider possible threats to the protected information and determine if the law covers the entire threat space, suggesting additional controls and policies where the law may be deficient.

## Scope of Project

In no less than 5 and no more than 10 pages prepare a report in PDF format with a font size of 10 points, single spaced, single column. Figures, tables, and the like are not included in the 10 page maximum page count, but text beyond the page limit will not be considered in grading. Quality of your analysis is more important than the quantity of words used!

The style of your report should be as if you were submitting it to senior management in a place you work as a security analyst. The report should not read as a research paper! Please submit the report on D2L.

## Academic Integrity

Completion of the semester project is to be an **independent, individual** effort for each student. Attempting to benefit from work of another student, past or present, and similar behavior that defeats the intent of an assignment is unacceptable to the University. Such behavior will be treated as a violation of USC academic integrity standards, which are summarized in the on-line tutorial available at the following web site:
https://viterbischool.usc.edu/academic-integrity/

## Description

The United States passed a law in 1996, the Health Insurance Portability and Accountability Act (HIPAA), later amended in 2003 (Privacy Rule) and 2013 (Security Rule and Breach Notification portions of the HITECH Act), which (among other things) was designed to govern the collection, disclosure, and protection of customers’ protected health information (PHI) by "covered entities" (such as health insurers and medical service providers) and other companies that may receive such information.

This project is based on a real-world business context. **Acknowledgement**: the documents used in this project were prepared by Dennis Maglinte - Bioinformatics Supervisor, Children's Hospital Los Angeles.

**Project context**: you are a cybersecurity professional working for a bioinformatics company – “the Center”. The company specializes in molecular pathology, clinical genetic labs, and research. The Center is a part of the Hospital and can be referred as “Hospital Center (HC)” in “HC-C04107_Data_Policies”.

The Center has a contract with another company – Cartagenia that provides a clinical informatics platform that the Center uses for data analysis. The Center's data is managed by a cloud provider - Amazon Web Services (AWS).

**Project-related documents** (posted on Piazza):

- **NIST-800-66r1.pdf**
  - Guidelines for implementing the HIPAA Security Rule
- **WhatIsConsideredProtectedHealthInformationUnderHIPAA.pdf**
  - Clarifies HIPAA requirements
- **CartageniaDataSecurityAndConfidentialityPolicy.pdf**
  - Illustrates issues around data ownership and security since data is stored in the cloud (AWS)
  - Cartagenia has an agreement with AWS and the Center has an agreement with Cartagenia
  - This document illustrates the legal aspect of responsibility
- **HC-C04107_DataPolicies.pdf**
  - Describes information protection policies that interpret HIPAA requirements. It also includes the description of measures that the Center takes to implement the policies. This interpretation is missing some important points outlined in the NIST-800-66r1. You need to add the missing requirements need to your report.
- **UsingGlobalUniqueIdentifiersToLinkCollections.pdf**
  - Description of the GUID system for de-identifying samples for complying with HIPAA and other regulations
- **AWS_HIPAA_Compliance_Whitepaper.pdf**
  - Outlines how companies can use AWS to create HIPAA-compliant applications
- **AWS_Disaster_Recovery.pdf**
  - Highlights AWS services and features for your disaster recovery processes to significantly minimize the impact on your data, your system, and your overall business operations

Your assignment is to write a report that summarizes the responsibilities the Center has for protecting patient data under HIPAA/HITECH and to make recommendations for a security policy that the Center should adopt to provide the necessary protection. Review NIST-800-66r1 to better understand how HIPAA requirements can be applied to the project. You can also search for helpful resources online.
For example, https://www.cerner.com/perspectives/protecting-hospital-from-cybersecurity-risks

You work must include the following:

**1.** Review the project related documents. Identify the information protection policies in them. Briefly summarize the policies that should be implemented (for example, "Members of the workforce will have the least amount of access necessary to PHI"). **Note: you should concentrate on the most important information security policies.**

2. Provide a summary of the potential threats to the protected information.

3. Convert the human-language policies (that you identified in Step 1) into access control policies suitable for implementing in an information management system.

   As discussed in class, when a policy is expressed in human language, inconsistencies and ambiguity are very common. For this project, you are free to interpret the policies as you see fit, just state your assumptions explicitly.

   a. Clearly identify users (subjects) and protected resources (objects). You can consider the subjects as various ***user groups*** or ***roles*** given in the Center policy document (HC-C04107_DataPolicies) like *root*, *bioinfo*, *bioinfoclin*, etc.

   b. Consider the applicability of DAC and MAC for both confidentiality and integrity, and suggest a **specific** mapping of labels and access structures (ACLs, capabilities, roles), as appropriate, to fully implement the most important access control policies. To implement MAC, you need to specify concrete object classifications, subject clearances, levels and categories. Make and clearly state any necessary assumptions that guided the selection of those attributes.

4. Identify other requirements (e.g., availability) that are not covered by the access control policies you developed in Step 3.

5. Identify the part of the threat space (that you determined in Step 2) your access control polices address and the part that they do not.

6. Recommend additional controls (e.g., administrative, physical) to cover the part of the threat space that your policies do not cover.

You may use web sites (e.g., https://www.hipaajournal.com/) and other aids to help you locate and interpret the privacy and security-relevant portions of the rather long and dry legal documents, but your report must be based on and reflect the actual wording of the law. Beyond the published documents and other on-line resources, you may enhance your understanding by 1) searching out a covered entity and interviewing them with respect to how they are implementing what they consider to be the HIPAA requirements; and 2) determining to what extent the covered entity is taking account of other dimensions to the threat space beyond the HIPAA requirements. **Be sure to cite your sources.**

## Grading

The semester project will account for 20% of the grade for the course. As detailed in class, there is a substantial grade penalty for late submission of a cumulative of 10% times number of days late, i.e., 1 day late loses 10%, 2 days 30%, 3 days 60%, greater than 4 days late not accepted.

The total of 100 points for the project will we allocated to three areas as follows:

1. [20 points] Familiarity with and analysis of the project-related documents, including information protection requirements and the threat space addressed.
2. [50 points] Systematic interpretation of the identified protection requirements in terms of access control policies, including MAC and DAC integrity and confidentiality.
3. [30 points] Conclusions and recommendations, including missing requirements and recommended enhancements.