COMPREHENSIVE MEDICAL SERVICES "CMS", is a highly advanced teaching and research hospital and medical facility that has gained notoriety around the world for its cutting edge technology and its high success rate in treating critically ill and severely burned patients. Currently there are three "branches" or "facilities" in the United States, located in Los Angeles, Saint Louis and Boston. Patients come from all around the world to receive treatment at one of the three CMS facilities and hospitals. The existing facilities share information between them. If for example a patient presents for treatment at the Boston facility on one visit, his medical providers and account representatives will have access to his personally identifiable information, prior medical diagnosis and treatment records, insurance, billing and payment history in real time regardless of which of the other facilities he has treated at previously. CMS is expanding its serves and will open a fourth facility in the southern United States. To that end, CMS as purchased a 10-acre tract of land just outside the city limits of Galveston, Texas. Other than purchasing the land and retaining an architect, CMS is still in the planning phase. It is CMS's intention to erect what will most likely be a 10 story structure in which CMS expects to house the hospital facility, doctor's offices, outpatient surgery center, administrative offices, management services which will include insurance, accounting (accounts payable and receivable included), loading docks for shipping and receiving, multiple parking facilities, and a data center.

Your team has been hired by COMPREHENSIVE MEDICAL SERVICES "CMS" to analyze and design a complete access control model for its new facility located in Galveston, Texas. The new Galveston facility should share information with the other three facilities, so that the patient information will be available in real time regardless of which facility the patient presents for treatment. Medical teams at all four facilities should be able to review the patients records and collaborate on the best course of treatment for it patients.

The complete access control model that you develop should be written in narrative form using the APA format. Please use ample subsections or subheading as appropriate. Your paper should have a 1-in margin on top, bottom, left and right margins. The paper should be double spaced. Use a cover page with a title, and the name of each team member who contributed to your project/paper. Each page should have a page number in the bottom right margin. The paper should also include a table of contents, that include subject headings, subheadings or subtopics, references or sources, and illustrations as well as page numbers for each.

For each major area or section of your model, which you will explain and justify in your paper, you should identify the options you considered in the form of a null and alternative hypothesis. Discuss the alternatives you considered, giving pros and cons of each, and prove information from the research you conducted that assisted you in arriving at your conclusion, or in establishing your hypothesis as to why one alternative was selected over another. You MUST cite the sources for your research any time you make reference to your research, whether that be through direct quotations or in summary. Your work should include no fewer than five (5) sources.

In addition to the written research paper that you will use to "sell" CMS on the access control model that you developed, when you present or "pitch" your model to CMS (and the rest of the class) you will use audio visual aids in the form of a Power Point presentation. Also use schematic diagrams, drawings, tables and illustrations where appropriate. For all diagrams, drawings, illustrations, and tables that you use or reference in your oral presentation and Power Point slides, please also include the same visual aids in the appendix of your written paper.

Your access control model should include, but is not limited to a discussion of the following:

4. What nature and extent of security that will be necessary for each of the systems or networks that you identify, including a discussion of things such as necessary firewalls.

5. For each or type of user identified which of the systems, databases, networks, and/or classes or types of information or data they will have access to. Include an explanation of why they do or do not have access to certain systems, networks, databases and types of information.

6. For each type or class of users discuss the type(s) and layer(s) of authentication that will be required, discussing the options available and why you made the authentication decision that you selected. Consider and discuss the logical access controls for your subjects as well as authentication factors.

7. Discuss the privileges that will be assigned to users, classes of users or types of users for each of your systems, networks and/or databases. Consider and discuss group access controls.

8. Discuss the classification schemes of information that will reside on your networks, systems and/or databases and explain the security classifications for each. Include how and when information may possibly be declassified.

9. Consider how and when information/data will be destroyed or disposed of at the end of its useful lifecycle. Also, consider the process of taking the computers, hard drives, and other physical components out of service at the end of their useful life.

10. Perform risk assessment for major components and discuss how you will handle risk for each major system/network/database. Consider and discuss alternatives and options for backup, mitigation of loss, loss prevention, and recovery. Explain why you chose one option over another.

11. Discuss and make recommendations for CMS's policies, standards, guidelines and procedures for information security. With regard to information security policies, demonstrate your critical thinking by developing an acceptable use policy for CMS that will describe what tasks can and cannot be performed using the organization's computing resources. Discuss the password policy, the account management policy and the remote access policy that you would recommend. While you will be unable to develop a complete set of standards needed to support CMS's policies, please highlight what you would consider the most significant standards and procedures that detail authentication, password management, and remote access. Discuss where you believe separation of duties, job rotation, and other policies are essential within the different departments or divisions of the organization in order to maximize security.

12. Discuss the alternative available and your recommendations for employee training regarding CMS's overall access control and security.

13. Don't overlook physical security! Discuss perimeter security and design a comprehensive plan for physical, building, parking structures, points of entry, creating physical obstacles and barriers that enhance security. Discuss the physical and logical placement of the data control center and its physical security. If you consider it beneficial use a schematic or drawing to illustrate physical security (and any other aspect of your access control model where illustrations, diagrams, or tables would enhance your explanation and/or presentation).

14. Consider biometric access controls for the different areas, systems, networks etc. that you have identified and discuss the alternative, explaining your recommendation and