

### **Health Care Scenario**

You have been asked by the Fresh Kills Clinic to evaluate their Electronic Medical Record System (EMRS) for HIPAA compliance. Below you will see a high level overview of the record system. The clinic is located in a single story building. It has 4 rooms. One room is the waiting area where patients first come and register. The second room is the nurses' station. This room is used to conduct a more detailed interview of the patient. The third room is the exam room where the doctor examines his/her patients. The fourth room is a server.

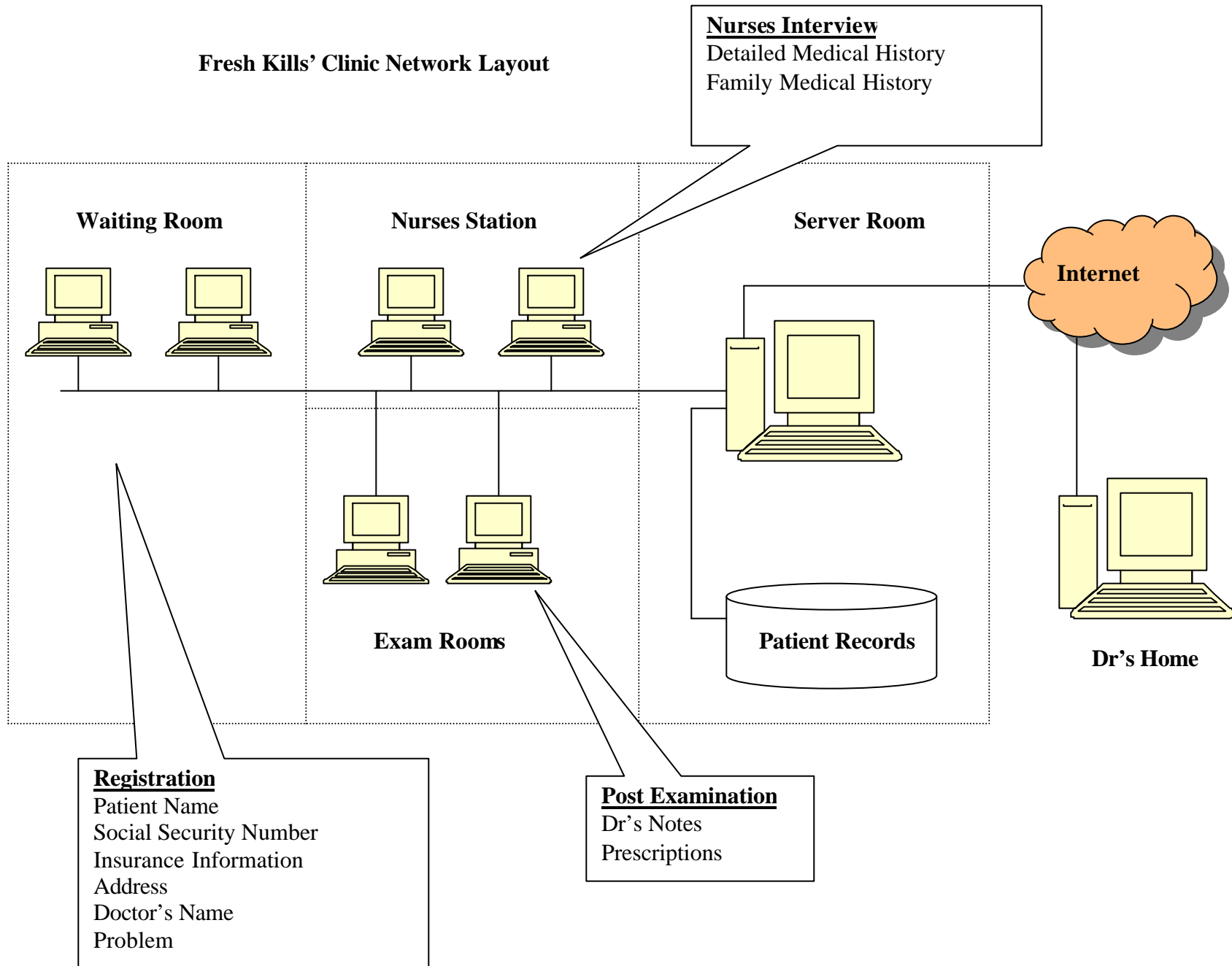
#### **A typical visit to the clinic involves the following:**

The patient arrives to the clinic and registers in the waiting room. They might have to wait to register since the clinic may have several patients. During the registration process the patient answers some basic questions about themselves. The receptionist enters the answers to the questions in the EMRS. The patient is then taken to a separate room, the nurses' station where they are asked more detailed questions about their medical history and their family's medical history. Afterwards, the patient is taken to an exam room where the doctor will examine them. Once the exam is over the doctor will enter any notes he has written as well as prescriptions that he has issued to the patient.

Throughout the process, information about the patient is being collected and stored in a patient record database (the information collected is detailed in the callouts in the diagram). The database is located in a separate room, the server room. This room is not locked and anyone can access it. To access the database one has to first go through a server. All workstations in the clinic are connected to this server. The server has no authenticated logon. Anyone can just come up to the server and log on. The server is also directly connected to the internet. The reason for this is that the doctors want to be able to work from home. They want to have access to patient's records so they can review their notes. **ALL** network traffic (internal and external) is in the clear.

Using the HIPAA requirements summary in the presentation, construct a list of 8 security requirements for this system that would be necessary to comply with HIPAA. For each requirement you list, give an example of a mechanism (VPN, Firewall, etc) that you would use to enforce this requirement.

**Fresh Kills' Clinic Network Layout**



**CS996-Information Security Management**  
**Homework: Legal Requirements**

**William Mendez**  
**March 25, 2004**