**NORTHEASTERN GENERAL HOSPITAL**

**Brief Description:**

This project is basically to monitor the flow of drug within the hospital and the doctor’s, pharmacist’s activities to protect the hospital from malicious activities with the help of Security Operating Centers.

**Actors:**

Hospital: System Admin, Admin, Doctor, Patient, Pharmacist

SOC: SOC Director, Tier1 Analyst, Tier2 Analyst

Use cases related to actors

1. Admin manages doctor, pharmacist and assigns patient doctor.
2. Patients SSN and card detail is captured along with other basic details.
3. When a doctor is assigned to a patient, doctor gets to see all information but SSN and credit card details.
4. Doctor prescribes patient and forwards the prescription to pharmacist and patient’s account electronically.
5. Pharmacist can see patient’s card detail and uses patient ID to cross verify patient when the patient goes to take medicines.
6. SOC director manages Tier1 and Tier2 analysts.
7. Tier1 analysts have time 0-15 min to decide and work upon threat vulnerability and create a case for the same.
8. If not decided for the threat vulnerability under 15 min by Tier1, automatically escalate the case to tier2.
9. Tier2 analyses and investigates the threat further.
10. Both analysts send reports to director so that he can analyze the information (if needed).

The user inquires the Personal Health Record system, based on the role the system provides the information specified by the permissions assigned to the user's role.

* Patients have the option to authorize the disclosure of their information…if they disclose...should be visible to everyone inside hospital if not disclosed then to certain doctor only.
* Log Management: Capture history of Doctors and pharmacist’s activities.
* Authorization failure more than two times blocks the user and its activities and should contact Tier1 analyst for reactivation.
* Tier1 analyst monitors malicious activities and blocks such activities.
* When adding a doctor…create access, assign devices and certificate for access for them.
* Keep strong password indication and change them regularly notification.
  + Minimum password length of 10 characters
  + Require passwords changes every 30 days
  + Inability to reuse the last 10 passwords
  + Utilize 3 out of four special characters such as numbers, lower case letters, upper case letters, or special characters
* Role based authorization: Based on their functional role, users can view(read), create, update, delete, or act (execute) on information contained in a patient's record.
* Context-based Authorization: right granted for a limited period to view those, and only those, records connected to a specific topic of investigation.