Alert Generator System

The Alert Generator System is an important subsection of the Cardiac Health Health Monitoring System. “DataStorage” is able to access patient records and patient data through the “DataRetriever” class. Moreover, it uses the “PatientIdentifier” class to associate the data it has just retrieved with a particular patient. This is critical to the Cardiac Health Monitoring System. It helps maintain the privacy and anonymity of patients while simultaneously allowing doctors and other medical personnel to identify individual patients and their status. The interfaces “DataStorage” and “PatientData” are bidirectionally associated as they constantly use each other to read and update patient records.

The “AlertGenerator” class uses “DataStorage” in order to have all patients’ most recent data and keep track of their vitals or status. “AlertGenerator” constantly evaluates the data from “DataStorage” against predetermined thresholds, dictated by medical protocols. As soon as the thresholds are reached, “AlertGenerator” creates an “Alert” object.

“AlertManager” is responsible for handling the “Alert” object. The “AlertManager” sends a message to staff on duty during the patient emergency through the “DirectMessage” class. The content of the message sent to employees is modelled through the “OutputStrategy” interface. The message delivers the following key points; the patient in distress (patientID), the time the alert was triggered (timestamp), the cardiac event the data are showing (label) and the patient’s vitals (data).

Data Storage System

A hospital system must hold a lot of data in order to adequately take of its patients. The Cardiac Health Monitoring System has a specialised subsystem dedicated to the secure storage of the sensitive patient data that the hospital procures daily. Within the Data Storage System, the interfaces “DataStorage” and “PatientData” are bidirectionally associated as they are critical in they collaborate in storing, updating and retrieving patient information, such as their IDs. Cybersecurity is critical within a hospital system in order to maintain the safety and privacy of their patients. Within the Data Storage System, security is ensured through the “DataStorage” class’ connection with “DataEncryption”

The process of how “DataStorage” retrieves data also illustrates the data security the Cardiac Health Monitoring System is built with. “DataStorage” uses “DecipherData” to decrypt the stored data. To be able to access the data, “DecipherData” uses the “SecuirtyCheck” class. Before the “SecurityCheck” class, users – hospital staff; doctors, nurses, and other authorised personnel – go through “UserAuthentication”. The authentication of the user utilising the Cardiac Health Monitoring System is handled by the “AuthenticationManager” class.

Patient Identifier

Data privacy, particularly medical data, is extremely important within a hospital setting. To ensure their patient’s privacy, the hospital generates a patient ID for each patient so that

their medical data is not readily associated with their personal data or their name. This can be seen through the way the Patient Identification System is built. The bidirectional relationship between “PatientIdentifier” and “PatientRecord” illustrates how the patientID is used to store the patient’s information; name, date of birth and medical history.
“PatientIdentifier” is also related to “IdentityManager” which further manages the relationship between data and the patient records within the Cardiac Health Monitoring System.

To provide the best medical care to each patient, doctors need to be able to identify the patient and personalise their medical care to their needs. To ensure that data and patient records are always up to date, the “PatientRecord” class is bidirectionally associated with the “DataStorage” interface. Together, they work to update and maintain pertinent patient information and ensure hospital records are accurate to the patient’s most current state.

“DataStorage” can participate in the editing of patient records, because the “DataStorage” interface uses the “PatientIdentifier” class to recognise which patient records to edit with the data it holds.

Data Access Layer

The Cardiac Health Monitoring System contains a lot of data. Therefore there is a whole subsection dedicated to how the data is safely accessed. Firstly, the interface “PatientData” uses “LegacySystems”. The “LegacySystems” class holds all the data stored in older and previously used databases within the hospital. “legacySystems” then uses the “FileDataListener” in order to read what data is being written and uploaded to “LegacySystems”. To then be able to perform operations on the data, the data is then passed through the “DataSourceAdapter”. The final processing of the data is completed by the “DataParser” class which uses the “DataSourceAdapter” class.
“DataListener” uses “DataParser” in order to feed the data to then “TCPDataListener” which is used by “SignalGenerator”. “SignalGenerator” uses the read data to generate signals when necessary. “SignalGenerator” also uses the “PatientIdentifier” class when generating the signals, as to indicate which patient the signal is related to.
“DataParser” is also used by the “WebSocketListener” which feeds the data collected into the “SecureWebPortal”. This is where medical personnel are able to access and interact with patient data, by using the “PatientRecord” class. Within the class all the relevant and pertinent patient information such as medical history name and date of birth (which indicates age) is available to them.