Case Scenario

An accredited hospital recruited healthcare staffs to start its operation. The hospital has an out patient department (OPD), consulting rooms and patients wards for inpatients. The hospital also has laboratory and radiology for medical tests and radiological services respectively. The hospital has various healthcare departments including Emergency department, Cardiology, Intensive care unit, Pediatric care unit, Cardiovascular care unit, ENT, Neurology, Oncology, Obstetrics and gynecology. A patient care involves nonemergency patient, appointment booking or walk in, to seek for medical care.

The patient reports at the OPD and got registered into the healthcare journal systems by the nurses or administrators. The registration involves the collection of the patient’s demographic data, vital signs and symptoms. The patient is further assigned to a medical officer for further assessment and diagnosis. The medical officer can request for laboratory tests and or radiology scans to support in taking medical decisions. A treatment plan is proposed to the patient. If the condition requires the patient to be hospitalized, a ward is assigned to the patient else, out patients may receive treatment and or collect drugs from the pharmacy and leaves. In patients received treatment in the hospital and is discharged after recovery. Another patient care path is through emergency situation. Emergency patients passed through the emergency department and followed the various steps while healthcare is provided.

Healthcare staffs are typically assigned to various work shift time and specific wards and patients. So, the healthcare professionals have the ability to access only patients records in which they have been assigned to. However, in emergency situations, the healthcare staffs can access the records of that patient under emergency without passing through conventional access authorizations. Additionally, a specialist from different hospital can be involve collaborating in patient care.

Security requirements

1. Access to personal health data and personal data filing systems for therapeutic purposes (including electronic patient records/data processing systems) must be granted following a specific decision based on the completed or planned implementation of measures for the medical treatment of the patient. Access must be controlled to ensure compliance with the confidentiality rules and so that no access to personal health data and personal data is given to anyone other than those with an official need to gain such access. In the case of the exchange of health data across organisations, both the organisations involved must have technical and organisational solutions which delimit access to health data which at least ensure that: • health data is not made available if the patient/health care user has objected or objects to it Code of conduct for information security and data protection in the healthcare and social services sector Version 5.3 30 • access is only given to health data which is relevant and necessary in order to provide, administer or quality-assurance health and social care services to the patient/health care user • the health personnel are authorized to gain such access and have authenticated themselves using a secure authentication solution[1, 2].
2. If provision is made for self-authorisation, technical measures must be established in such a way that health personnel may gain access to personal health data and personal data as and when necessary. Such access must be justified and registered in personal

health data and personal data filing systems for therapeutic purposes (including electronic patient records).

1. The misuse of self-authorization must be followed up as a breach
2. Systems that administer authorization must distinguish between rights to read, register, correct, erase and/or block personal health data and personal data. All allocations of authorization must be registered in a register of authorizations.
3. At least the following must be recorded in the logs: • unique identifier for the authorised user
   * the role of the authorised user at the time of access
   * organisational affiliation
   * organisational affiliation of the authorised person
   * type of data to which access has been gained
   * who disclosed health data that is linked to the name or national ID number of the patient or health care user
   * basis for the access
   * time and duration of access.

**Research questions**

Based on the above scenarios, how can healthcare professional’s security practice be observed in the access logs of the electronic health records

Hypothesis

1. Normal security practice would pass through conventional authentication and authorizations procedures

Normal:

Rule based:

1. The logDateTime is between the shiftStartTime and shiftEndTime
2. The employeeDepartmentID and the patientDepartmentID are the same
3. ipAddress is the hospital ipAddress
4. osID, deviceID, and browserID is the same OS the employee uses everyday

Data driven:

1. the time difference between the logDateTime and the shiftStartTime
2. the time difference between the logDateTime and the shiftEndTime
3. the same department/not (0/1)

100 records: 80 training data

model

20 testing data

1. Emergency accesses may use break the glass access control mechanisms but only in an actual emergency situation in the given date and time of the reported emergency case
2. Anomaly security practice can occur when a healthcare staff accesses patient outside their shift ward or category of patients in their shift period
3. Anomaly may also occur when a staff access more than average dataset in comparison to average accesses of similar colleagues
4. Anomaly can also occur if there was access of patients data through break the glass access control when the patient was not under emergency care.
5. If there were irregular role activities. For instance, a nurse performing roles of a doctor, pharmacist, laboratory technicians etc.

**List of objects**

Healthcare requirements

1. Roles(RoleID, RoleType)
2. Staff(StaffID, FirstName, Surname, OtherNames, RoleID, Gender, Dateof Birth)
3. Department(DepartmentID, DepartmentName, Description)

1. Yeng P., Yang B., Snekkenes E., editors. Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC); 2019 15-19 July 2019.

2. Code of conduct for information security and data protection in the healthcare and care services sector, (2018).