Work flow based anomaly detection using Electronic Health Records (EHR) logs

Introduction

Related work

Scope and contribution

Our method

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 book appointment with the General Practitioner (GP) and got registered into the healthcare journal systems by the nurses. The registration involves the collection of the patient’s, 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 further attention, the patient is referred to the hospital or the specialist care.

At the hospital if the patient condition require observation, the patient is hospitalized and for that matter, a ward is assigned to the patient. The In patients received treatment in the hospital and is discharged after recovery. Another patient care path into the hospital is through emergency situation. Emergency patients passed through the emergency department and followed the various steps while healthcare is provided. The specialist care such as Ear Nose and Throat(ENT) and Eye, may be in the hospital or outside the hospital.

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).
3. The misuse of self-authorization must be followed up as a breach
4. 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 authorisations.
5. 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.

1. Confidentiality must include the following:
   * Persons outside the organisation must not be able to gain unauthorised access to personal health data and personal data.
   * Persons within the organisation must be given access in accordance with established principles for access control
   * The names of persons who have had access must be recorded in logs in personal health data and personal data filing systems (including electronic patient records (EPR)) and data processing systems.
2. **Integrity**
   * The names of persons who entered records, changes, corrections and deletions must be recorded in personal health data and personal data filing systems for health purposes (including electronic patient records (EPR)) and data processing systems. This will ensure that there is an audit trail to the origin.
   * Security measures must be implemented to ensure that persons or technology, either within or outside the organisation, must not be able to change personal health data and personal data without authorisation.
   * Personal health data and personal data must be accurate and be linked to the appropriate identified person.
3. **Availability** 
   * Within the framework of the duty of confidentiality, personal health data and personal data must be accessible when there is an official need to access such data.
   * Self-authorisation may be established as an option for authorized users to give themselves access without following established principles for gaining access to personal health data and personal data in accordance. In such cases, specific procedures must be prepared. The reason for self-authorisation must be documented.
   * The misuse of self-authorisation must be followed up as a breach.

**Research questions**

Base 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
2. Anomaly may also occur when a staff access more than average dataset in comparison to average accesses of similar colleagues having pass through conventional authentication and authorizations procedures
3. 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
4. Anomaly security practice can occur when a healthcare staff accesses patient outside their shift ward or category of patients in their shift period
5. 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.
6. If there were irregular role activities. For instance, a nurse performing roles of a doctor, pharmacist, laboratory technicians etc.

Observing in logs

1. Who access a record for what and when
2. Check of interorganizational accesses eg check ip address, organization ID,
3. Check if there was consent to access record eg check if there was agreed referral
4. Check for minimum and necessary access: how
5. Check abuse of self-authorization eg if there was a complete or a planned implementation of measures for the medical treatment of the patient, check activities of the access of the patient record
6. How to observe unauthorized accesses: failed login attempts, accesses outside therapeutic plans, average number of records accessed in comparison with the user group communty