Syrian Arab Republic

Ministry of Higher Education

Syrian Virtual University

EHR-Hospital

Students:

Name	ID	Class
Ali Hassan	Ali_112862	C1
Eissa ALNissani	eissa_114377	C2
Rami Shehan	rami_110878	C1

Project done under supervision of doctor Moutasem Shafamry

For the WIS model in the MWT course at the SVU

Content

Introduction……. 1

Electronic Health Record (EHR)…… 2

EHR Standards……. 3

EHR Users and Authorities……..……... 5

EHR Services and Infrastructure…….. 8

EHR Requirements and System Model…… 10

The Application…… 14

List of References……. 16

Tables……. 17

Introduction

Over the past 20 years, the world has undergone a major transformation due to information technology (IT). Today, we have at our fingertips access to a variety of information and services to help us manage our relationships with the organizations that are part of our lives: banks, utilities, government offices — even entertainment companies.

Although it will take years for health care to realize all these improvements and fully address any pitfalls, the first changes in this transformation are already underway. At the same time, numerous technology tools are becoming available to improve health for you, your family, and your community.

Most consumers will first encounter the benefits of health IT through an electronic health record, or EHR, at their doctor's office or at a hospital.

Benefits of Health IT

- EHRs reduce your paperwork. The clipboard and new patient questionnaire may remain a feature of your doctor's office for some time to come. But as more information gets added to your EHR, your doctor and hospital will have more of that data available as soon as you arrive. This means fewer and shorter forms for you to complete, reducing the health care "hassle factor".
- EHRs get your information accurately into the hands of people who need it. Even if you have relatively simple health care needs, coordinating information among care providers can be a daunting task, and one that can lead to medical mistakes if done incorrectly. When all of your providers can share your health information via EHRs, each of them has access to more accurate and up-to-date information about your care. That enables your providers to make the best possible decisions, particularly in a crisis.
- EHRs help your doctors coordinate your care and protect your safety. Suppose you see three specialists in addition to your primary care physician. Each of them may prescribe different drugs, and sometimes, these drugs may interact in harmful ways. EHRs can warn your care providers if they try to prescribe a drug that could cause that kind of interaction. An EHR may also alert one of your doctors if another doctor has already prescribed a drug that did not work out for you, saving you from the risks and costs of taking ineffective medication.
- EHRs reduce unnecessary tests and procedures. Have you ever had to repeat medical tests ordered by one doctor because the results weren't readily available to another doctor? Those tests may have been uncomfortable and inconvenient or have posed some risk, and they also cost money. Repeating tests—whether a $20 blood test or a $2,000 MRI (in the USA) – results in higher costs to you in the form of bigger bills and increased insurance premiums. With EHRs, all of your care providers can have access to all your test results and records at once, reducing the potential for unnecessary repeat tests.
- EHRs give you direct access to your health records. In the United States, you already have a Federally guaranteed right to see your health records, identify wrong and missing information, and make additions or corrections as needed. Some health care providers with EHR systems give their patients direct access to their health information online in ways that help preserve privacy and security. This access enables you to keep better track of your care,

and in some cases, answer your questions immediately rather than waiting hours or days for a returned phone call. This access may also allow you to communicate directly and securely with your health care provider.

Until now, almost no one in our country has had the opportunity to use this kind of technology to enhance some of the most important relationships: those related to your health. Relationships with your doctors, your pharmacy, your hospital, and other organizations that make up your circle of care are now about to benefit from the next transformation in information technology: health IT. For patients and consumers, this transformation will enhance both relationships with providers and providers' relationships with each other. This change will place you at the center of your care.

I- Electronic Health Record (EHR)

As defined by The Office of the National Coordinator for Health Information Technology (ONC) at the USA, EHRs are at their simplest, digital (computerized) versions of patients' paper charts. But EHRs, when fully up and running, are so much more than that. EHRs are real-time, patient-centered records. They make information available instantly, "whenever and wherever it is needed". And they bring together in one place everything about a patient's health. EHRs can:

- Contain information about a patient's medical history, diagnoses, medications, immunization dates, allergies, radiology images, and lab and test results.
- Offer access to evidence-based tools that providers can use in making decisions about a patient's care.
- Automate and streamline providers' workflow.
- Increase organization and accuracy of patient information.
- Support key market changes in payer requirements and consumer expectations.

One of the key features of an EHR is that it can be created, managed, and consulted by authorized providers and staff across more than one health care organization. A single EHR can bring together information from current and past doctors, emergency facilities, school and workplace clinics, pharmacies, laboratories, and medical imaging facilities.

Electronic Health Records (EHRs) have been widely adopted over the past decade in both inpatient and outpatient settings. EHR systems are made up of the electronic patient "chart" and typically include functionality for Computerized Provider Order Entry (CPOE), laboratory and imaging reporting, and medical device interfaces. Ideally, the system creates a seamless, legible, comprehensive, and enduring record of a patient's medical history and treatment. However, the transition to this new way of recording and communicating medical information has also introduced new opportunities for error and other unanticipated consequences that can present safety risks.

In a review of EHR safety and usability, investigators found that the switch from paper records to EHRs led to decreases in medication errors, improved guideline adherence, and (after initial implementation) enhanced safety attitudes and job satisfaction among physicians. However, the investigators found a number of problems as well. These included usability issues, such as poor

information display, complicated screen sequences and navigation, and mismatch between user workflow in the EHR and clinical workflow. The latter problems resulted in interruptions and distraction, which can contribute to medical error. Additional safety hazards included data entry errors created by the use of copy-forward, copy-and-paste, and electronic signatures, lack of clarity in sources and date of information presented, alert fatigue, and other usability problems that can contribute to error. Similar findings were reported in a review of nurses' experiences with EHR use, which highlighted the altered workflow and communication patterns created by the implementation of EHRs.

II- EHR Standards

The (ISO 18308:2011) is considered the main standard when studying the requirements and the implementation of an EHR system and it states:

1- Requirements for the representation of clinical information

a. **Kinds of health record entries:** the different types of data values and data entries that are needed to be allowed by an EHR (text, time and duration, drawings, diagrams, charts, tables...).
b. **Structure of health record entries:** the different aspects of records that are either mandatory or optional in an EHR (Longitudinal partitions of a health record, Multiple values of the same measurement, Data that were originally represented as a table such that the logical relationships of the data to row and column headings are preserved…).
c. **The representation of context within the health record entries:** The EHR may enable the representation of all types of entries according to the context of clinical care (Clinician's comment, Rationale for clinical decisions, Enable an author to explain or justify his or her reasoning or assertions, Optionally to reference external sources as the basis for a conclusion or strategy…).
d. **Intra-record links:** The EHR must be able to connect different sections of health records through links so that a whole longitudinal health record is formed (Defined and labelled relationships, Relationship between one or more health record entries connected through changes in the life cycle status of an activity or plan, Preexisting health record entry to a newer entry…).
e. **The representation of data values within health record entries:** the following types of data values are to be included in the EHR architecture (textual entries, terms, quantity and numeric data, time, Boolean data, graphical and multimedia data, externally referenced data).
f. **EHRA data retrieval and views:** The EHR may enable the representation of different ways of data retrieval for multiple views of the same data (Filtering or selective retrieval for entries, Authorized analysis within an individual subject of care's record and on a population of records, Chronological overview of the entire EHR for a subject of care…).

g. **Representation and support of clinical processes and workflow:** The EHR may be able to represent the progression of care in clinical practice under the following headers (Support for clinical processes and workflow, Decision support, guidelines, protocols, Care planning, Support of orders and services, Integrated care, Quality assurance).

2- Communication and interoperability requirements:

communication between different departments of one organization and between different organizations also.

3- Ethical and legal requirements: The EHR may

a. Represent and persist all information relevant to supporting and improving the wellness, health and healthcare of the subject of care.
b. Represent all the information included by an authorized clinician/professional.
c. Involve the details of one subject of care (Unambiguously), along with the details of his /her care takers (family members announced by subject of care).
d. be able to consider one or more than one identifier for a subject of care.
e. The EHRA may uniquely and reliably identify users who author or authorize entries in a health record (i.e. who have determined the information to be entered into an EHR).
f. It may identify the parties who enter data into the EHR.
g. The EHR may record the location of the hospital where the data was recorded regarding the clinical care of the subject.
h. Record the date and time at which each health record entry was originally committed to an EHR repository.
i. Record the date and time when the event documented occurred
j. Record the date and when the documented information was submitted to EHR repository.
k. Identify each and every entry in the data as the new version and save the previous data as the previous version.
l. Identify the prior version that was the source of a revision of an EHR entry.
m. Represent the rationale for revising an EHR entry or set of entries.

4- Fair Information Principle:

a. **Accountability:** The EHR may be able to recognize the organization which is either the source of information or is involved in the communication of the information to other organization and EHRA may be able to represent it.
b. **Identifying purposes:** It may identify various purposes for which the data versioning happened, or the data was collected by any person.
c. **Consent:** EHRA may be able to represent consent for new data entry, disclosure of data, transfer of data and its tracking details.

d. **Limiting collection, use, disclosure, retention:** EHRA may enable the implementation of policies that control access for use and access for onward disclosure of EHR information to authorized individuals and computer systems.
e. **Access policies:** The EHRA may be able to represent the access of the user to his/her data and should allow the user to specify policies for the access of the concerned data. It should be able to update the policies when and where ever required.
f. **Subject access:** The EHRA may be able to represent the changes to EHR information made by subjects of care or their legal representatives to correct errors, including amendments to the disclosure policy for entries.
g. **Auditability:** EHRA may enable the maintenance of an audit trail of the creation of, amendment of, and access to health record entries. EHRA audit trail may be protected from modification.

III- EHR Users and Authorities

Health and care environments increasingly comprise complex networks of agencies and actors from traditional healthcare settings, social care, informal carers and voluntary agencies (such as welfare charities) patients themselves, families and sometimes their social networks. All of these might at times establish agreements to permit data sharing of personal health data. Given the dynamic nature of this "virtual care team" it might not be practical for these data sharing agreements to be negotiated in traditional human to human document-based ways. It is therefore likely that such agencies will establish framework agreements that specify in advance the standards they each comply with, any mappings between their respective domains of privilege and how data are to be handled within each such privilege domain. As stated above, this policy model permits jurisdictions to instead declare alternative term lists that they will use. This allows for some flexibility in adoption of this document, recognizing that complex data sharing environments might need to establish new, potentially richer, vocabularies to describe the wider range of actors and roles in that environment.

A number of existing and legacy systems might not be able to incorporate richly-defined policy specifications, and many healthcare regions might not be in a position to define such policies for some years. Therefore, as a complement to the overall policy model in Clause 7, this document defines two vocabularies that can provide a minimum basis for making an access policy decision, and ensure a basic level access policy interoperability, albeit at a coarse-grained level.

These two vocabularies are:

a) a sensitivity classification of EHR data (at the level of COMPOSITION)

b) a high-level classification of EHR Requesters and Recipients, through a set of Functional Roles.

Within many healthcare environments (within and between collaborating healthcare teams involved in the direct provision of care to patients) the norm is to share health record information openly. It is indeed the wish of the vast majority of patients that teams do this, and many patients are actually surprised at how little of their health record is shared today when it should be, for safety and for good continuity of care.

Few contemporary healthcare systems (on paper or electronically) define complex internal access control partitions to the health records that they hold. Even if it were considered useful to define numerous fine-grained access policies, in practice it might take health care systems, national health services and millions of patients quite a long time to specify suitable access control policies for all of their EHR data, and to implement software components that can perform many complex policy-bridging computations in real time. Maintenance of these policies as the clinical care requirements of each patient evolve would also be a complex process.

Whilst a suite of access policies might in theory be defined (by patients or by others) to provide a multi-level access level framework within any given EHR, in practice most clinical settings operate on the basis of default privileges granted throughout the health record to any healthcare or health-related professional who has a legitimate interest in that patient. (The definition of who has such a legitimate interest will vary between organizations, and is not the scope of this document.) However, it is also well accepted that patients and professionals might at times need to restrict access to some more personally-sensitive EHR data. It is also common in most health services to ring-fence certain clinical settings as having exclusive portions of an EHR (for example, sexual health clinics). And whilst a set of rich policies might be defined for specific kinds of patients, specific settings, or just because one patient is more concerned about his or her EHR than another, the adoption of distributed EHR solutions needs to be managed on the basis that a sensible set of defaults and a simple framework will satisfy the majority of cases in the near future. This is because a rich set of policies might not be capable of direct interpretation and incorporation within the EHR system of an EHR Recipient, even if the information in those policies can be communicated in a standardized way.

For simplicity, we have considered role as a class. we can basically consider seven types of roles. Our aim is to categorize or group the patient's EHR according to these classes. Medical data are grouped according to role (class) authority. As the authority of the role is modified, the data of the concerned class automatically change. We have considered seven possible classes. One and only one class is associated with each user. Here we will discuss each of them. However, there can be other classes that are not included in this work (in table-1- we can see the feature values with respect to user role).

1- General Doctor

The user Doctor is a patient's nominated doctor/physician, who works as a family doctor or primary doctor responsible for admitting, attending, consulting or refereeing other doctor/physician in the EHR system. We assume that the doctor has authority to access all the patient data. The Doctor class contains data that are accessible to the doctor only. In case of doctors, there is one large class that will contain all information of the patient.

2- Referee Doctor

This user is any specialist doctor of particular diseases, to whom the patient's nominated doctor has referred. Since they are consigned doctors, they have less authority of patient's EHR. There is some sensitive information about the patient that need not to be shared with the referring doctor; meaning except sensitive information of patients, all EHRs of the patient are accessible to the referee doctor. Sensitive information is HIV information, mental disorder information, some sexual disorders, etc. When a referee doctor logs into the system, the underlying data access control system automatically groups all the EHR except sensitive information. Now this group of data is called 'Referee Doctor class'.

3- Nurse/Ward staff

A nurse is a person who is trained to give care to people who are sick or injured. Nurses work with doctors and other care workers to make patients well and to keep them healthy. A nurse monitors vital signs such as BP, temperature, pulse, etc., and records it. He or she provides frequent patient evaluations, including monitoring vital signs and performs essential procedures. There are two kinds of data that can be accessed by the nurse: -1-sensor collected data -2-patient's abstract general information. So, the features of these data may be pulse rate, heart rate, temperature, SPO2, BP, name, age, city, live status, etc. According to the above features the system will classify the data.

4- Relative

The relative is a person who is most closely related to a patient and nominated by the patient to make decisions on his or her behalf if he or she is unable to make any decision. Mostly he or she is authorized to access all the personal information of the patient as well as all insurance-related information. Since he or she is a non-professional, there is no need for him or her to access the patient's EHR.

5- Administrative staff

The administrative staff are people who are responsible for the smooth operation of the hospital or doctor's clinic. They are behind-the-scene support staff in the hospital who do the billing and provide some help to patients. They are just authorized to access the personal information and insurance-related information. Sometimes they also include ward staff or receptionist.

6- Patient

The patient is a person who requires healthcare services. The patient is owner of his or her EHR, has need of medical treatment by a doctor, nurse or other healthcare provider and has at least one EHR in the medical database. The patient is authorized to full access of his or her EHR by default

7- Insurer

The insurer is an insurance company which pays for the patient's treatment. Insurance companies will not have access to EHRs unless they have the consent of the consumer. They can just take the prescription of the patient from the doctor.

There are other classes that can be thought of such as pharmacists, clinics, labs … but as long as we are focused in this work on a system for only one hospital then the above can be considered as satisfactory.

IV- EHR Services and Infrastructure

Our world has been radically transformed by digital technology – smart phones, tablets, and web-enabled devices have transformed our daily lives and the way we communicate. Medicine is an information-rich enterprise. A greater and more seamless flow of information within a digital health care infrastructure, created by electronic health records (EHRs), encompasses and leverages digital progress and can transform the way care is delivered and compensated. With EHRs, information is available whenever and wherever it is needed and this provided many advantages and services:

1- Improved Patient Care

- **a.** Quick access to patient records from inpatient and remote locations for more coordinated, efficient care
- **b.** Enhanced decision support, clinical alerts, reminders, and medical information
- **c.** Performance-improving tools, real-time quality reporting
- **d.** Legible, complete documentation that facilitates accurate coding and billing
- **e.** Interfaces with labs, registries, and other EHRs
- **f.** Safer, more reliable prescribing

2- Increase Patient Participation

- **a.** Ensure high-quality care. With EHRs, providers can give patients full and accurate information about all of their medical evaluations. Providers can also offer follow-up information after an office visit or a hospital stay, such as self-care instructions, reminders for other follow-up care, and links to web resources.
- **b.** Create an avenue for communication with their patients. With EHRs, providers can manage appointment schedules electronically and exchange e-mail with their patients. Quick and easy communication between patients and providers may help providers identify symptoms earlier. And it can position providers to be more proactive by reaching out to patients. Providers can also provide information to their patients through patient portals tied into their EHR system.

3- Improved Care Coordination

Electronic health record (EHR) systems can decrease the fragmentation of care by improving care coordination. EHRs have the potential to integrate and organize patient health information and facilitate its instant distribution among all authorized providers involved in a patient's care. For example, EHR alerts can be used to notify providers when a patient has been in the hospital, allowing them to proactively follow up with the patient.

With EHRs, every provider can have the same accurate and up-to-date information about a patient. This is especially important with patients who are:

a. Seeing multiple specialists
b. Receiving treatment in emergency settings
c. Making transitions between care settings

4- Improved Diagnostics & Patient Outcomes

When health care providers have access to complete and accurate information, patients receive better medical care. Electronic health records (EHRs) can improve the ability to diagnose diseases and reduce—even prevent—medical errors, improving patient outcomes. A national survey of doctors1 who are ready for meaningful use offers important evidence:

a. 94% of providers report that their EHR makes records readily available at point of care.
b. 88% report that their EHR produces clinical benefits for the practice.
c. 75% of providers report that their EHR allows them to deliver better patient care.

5- Practice Efficiencies and Cost Savings

Many health care providers have found that electronic health records (EHRs) help improve medical practice management by increasing practice efficiencies and cost savings. EHRs benefits medical practices in a variety of ways, including:

a. Reduced transcription costs
b. Reduced chart pull, storage, and re-filing costs
c. Improved documentation and automated coding capabilities
d. Reduced medical errors through better access to patient data and error prevention alerts
e. Improved patient health/quality of care through better disease management and patient education

• Hardware needs

The right hardware can save an organization time and money. Some clinics find that a printer in every room saves 30 minutes of physician time per day and a large monitor saves 20 minutes of physician time per day. Furthermore, some practices reduce the time spent logging into the system multiple times each day by providing every worker with their own laptop or tablet to carry from room to room. System hardware (i.e., server and network) needs depend on the type of EHR purchased Physician practices may hire an IT service company to help them with their system hardware needs. Typically, IT service companies are independent from the EHR vendor and may not even specialize in the health care industry. Both the IT service company and EHR vendor can be helpful in finding the right

equipment at the best possible price. The IT service company may also supply, install and troubleshoot all devices, including the local.

V- EHR Requirements and System Model

One theme of the literature on EHR implementation is the emergence of unanticipated consequences. For example, a detailed study of types and rates of medication safety events before and after EHR implementation in two ICUs found that, while overall medication safety improved, new vulnerabilities emerged, including increases in wrong patient, wrong medication, or wrongly timed orders. One source of technology-induced error was overspecification of functions within the CPOE module. In the ICU study, the CPOE system required physicians to select the medication schedule, a function that nurses or pharmacists may be better prepared to do (and had historically done) in inpatient settings. Similarly, in a case study of electronic prescribing for patients with diabetes in a safety net clinic, investigators found overspecification to be a source of medication errors in both insulin ordering and insulin use. Specifically, when prescribers were forced by the CPOE system to select brand name insulin from a list of similar-looking brand names, they could inadvertently choose an incorrect type of insulin. The system configuration also presented barriers to pharmacist consultation on insulin selection, reducing opportunities for preventing or correcting prescription errors. A review of studies of EHR issues that present patient safety risks found numerous problems with software functionality and usability (Table-2-). A review of studies conducted in 2014–2015 found safety gains associated with EHRs and other health information technology (IT), but also determined that these systems have yet to live up to their full potential. Furthermore, confusing interfaces and security measures have disrupted workflow and communication and created incentives for clinicians to develop unsafe workarounds. Guidelines and frameworks for safe health IT implementation and use have been developed. However, several experts have observed that the present state of EHRs represents a "big miss," in that they have failed to appreciate and account for the complexity of patients and health care processes; the depth of cognitive work, communication, and collaboration required to optimally support the work of health care; and the cognitive load created by the poor usability of current systems. These experts envision a future in which user-centered design and fundamental rethinking of how EHRs can and should work will allow these systems to reach their full potential, ultimately transforming health care to achieve higher value and a more satisfying experience for patients and clinicians. Another requirement that should be talked about and focused on is staff training.

All requirement for an EHR architecture stated by the International Standardization Organization (ISO 18308) are listed in figure-1- below.

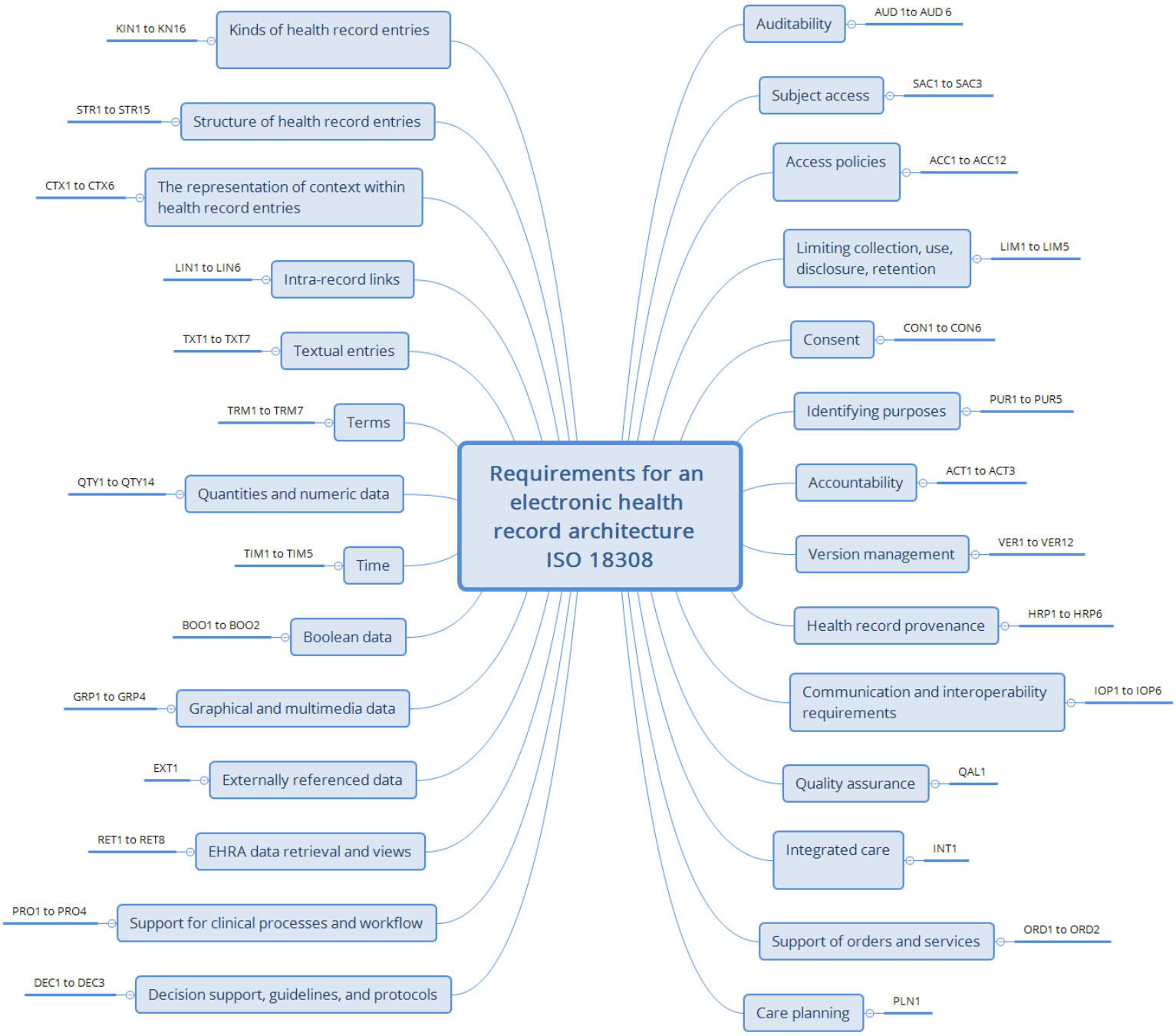


Figure-1- Requirement for an EHR architecture

Generic healthcare security requirements:

The most widely accepted requirements for an overall security approach in domains handling sensitive and personal data are published in ISO/IEC 27002. This specifies the kinds of measures that should be taken to protect assets such as EHR data, and ways in which such data might safely be communicated as part of a distributed computing environment. A health specific guide to this general standard has been published in ISO 27799 (Health informatics – Security management in health using ISO/IEC 27002). This will facilitate the formulation of common security polices across healthcare, and should help promote the adoption of interoperable security components and services. ISO 22600 (Health informatics — Privilege management and access control) defines a comprehensive architectural approach to formally and consistently defining and managing such policies. For EHR communication across national borders ISO 22857 provides guidance that can be used to define appropriate security policy specifications.

The exact security requirements that need to be met to permit any particular EHR communication instance should be governed by a number of national and local policies at both the sending and receiving sites, and at any intermediate links in the communications chain. Many of these policies will apply to healthcare communications in general, and will vary between countries and clinical settings in ways that cannot and should not be directed by this document. The approach taken in drafting this document has therefore been to assume that generic security policies, components and services will contribute to a negotiation phase (the access decision) prior to sanctioning the communication of an EHR Extract, and will protect the actual EHR data flows.

The ISO documentations therefore requires that an overall security policy or set of policies conforming to ISO 27799 is in place at all of the sites participating in an EHR communication, and also that these policies conform to national or trans-border data protection legislation. Additional polices might be required to conform to specific national, local, professional or organization regulations applicable to the communication or use of EHR data. Defining such policies is beyond the scope of this document.

Relationship to other related security standards:

Legitimate access to EHR data will be determined by a wide range of policies, some of which might exist as documents, some will be encoded within applications, and some within formal authorization system components. It is recognized that vendors and organizations differ in how they have implemented access control policies and services, and the extent to which these are presently computerized.

ISO 22600 (all parts) defines a generic logical model for the representation of the privileges of principals (entities), of access control policies that pertain to potential target objects, and of the negotiation process that is required to arrive at an access decision. Figure 2 depicts the concepts of Role Based Access Control defined in ISO 22600 (all parts).

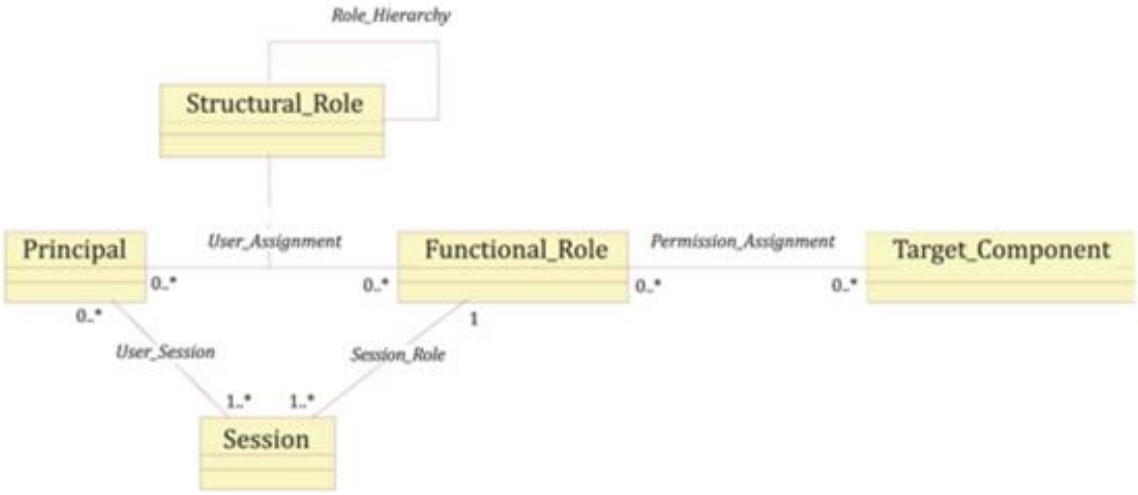


Figure 2 — Main concepts and policy types defined in Role Based Access Control [ISO 22600 (all part)]

And defining constraints on roles, processes, target objects and related privileges by policies, Figure 2 turns into Figure 3, according to ISO 22600 (all parts).

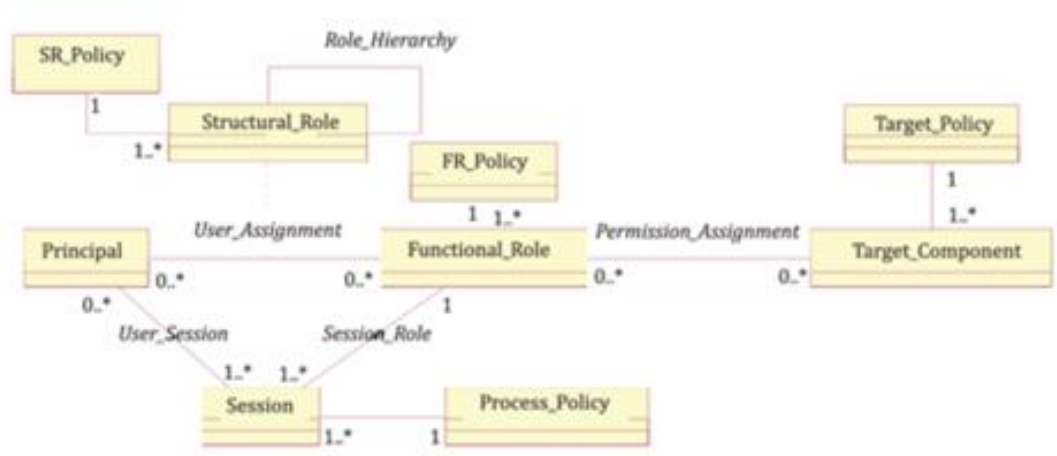


Figure 3 — Policy-driven RBAC Schema

As illustrated in Figure 3, principals (persons, agents etc.) are mapped to one or more Functional Roles, which will be influenced by the Structural Roles that they are permitted to hold. For example, a person who is medically qualified and a specialist in child health might hold one or more Structural Roles (such as Consultant Pediatrician at a hospital, Head of Child Screening for the region). Those Structural Roles might permit him or her at times to act with the Functional Role of Personal Clinician to a patient. The Functional Role might be persistent, or limited to a single user session. Functional

Roles are mapped to permissions to perform particular operations (such as writing new entries in an EHR) and to particular objects (such as the EHR data which that role-holder is permitted to view).

For the purposes of this document, the Target Component class shown in Figure 3 is the EHR data held by the EHR Provider. The Permission Assignment association defines policies to permit or deny access to part or all of the EHR, which need also to be communicated to the EHR Recipient for onward adoption and propagation. Whilst this document assumes the adoption of that standard it is acknowledged that national operational structures and terminology will differ and that variances will be possible. However, this document only specifies the policy model as a framework to communicate actual access policies in an interoperable way. It does not itself define the content of the access policies that are to be determined at jurisdictional or more local levels.

As a complement to that standard, ISO 21298 define sets of Structural Roles and Functional Roles that can be used internationally to support policy negotiation and policy bridging (for example during the negotiation phase of an access decision). This document also assumes the adoption of that standard, and aligns with it.

The relationship of the policy model defined in this document to the HL7 Healthcare Privacy and Security Classification System is explained in Annex B.

ISO 27789 defines a comprehensive representation of audit log and audit trail information relating to all of the events that might occur within electronic health record systems. This includes the communication of EHR data between repositories and systems. This document assumes conformance to that standard, and defines a profile (sub-set) of the ISO 27789 audit log model specifically for the purpose of communicating with patients and other authorized parties' information about who has accessed the EHR of a specified patient, when and why.

A large number of EHR-specific medico-legal and ethical requirements are expressed within ISO 18308, although compliance with these is primarily met through specific classes and attributes of the EHR Reference Model (published in ISO 13606-1). The ISO 13606 standard as a whole enables conformance to ISO 18308, and this document specifically enables conformance to its ethical and legal requirements and fair information principles.

VI- The Application

As we can see in the theoretical study above, the issue of the "right" way to implement or secure the medical systems based on EHR is still a dilemma, and even international organizations have different views and concerns, especially when all different possible sets and environments are taken into consideration. And as the case is much different and harder here in Syria, we contacted doctors and residents at Tishreen University Hospital to build an application that is somewhere in between the international standards of EHR and the known protocols at the Syrian hospitals, and the main reason we didn't stick to the standards only is because we believe that it wont be affective to ask medical staff of a hospital to move to an automated system and to change their work protocol at the same time, and here we find it necessary to mention two points: first, the importance of staff training has a greater value in such case(Syria), and second, the main difference between the Syrian hospitals and

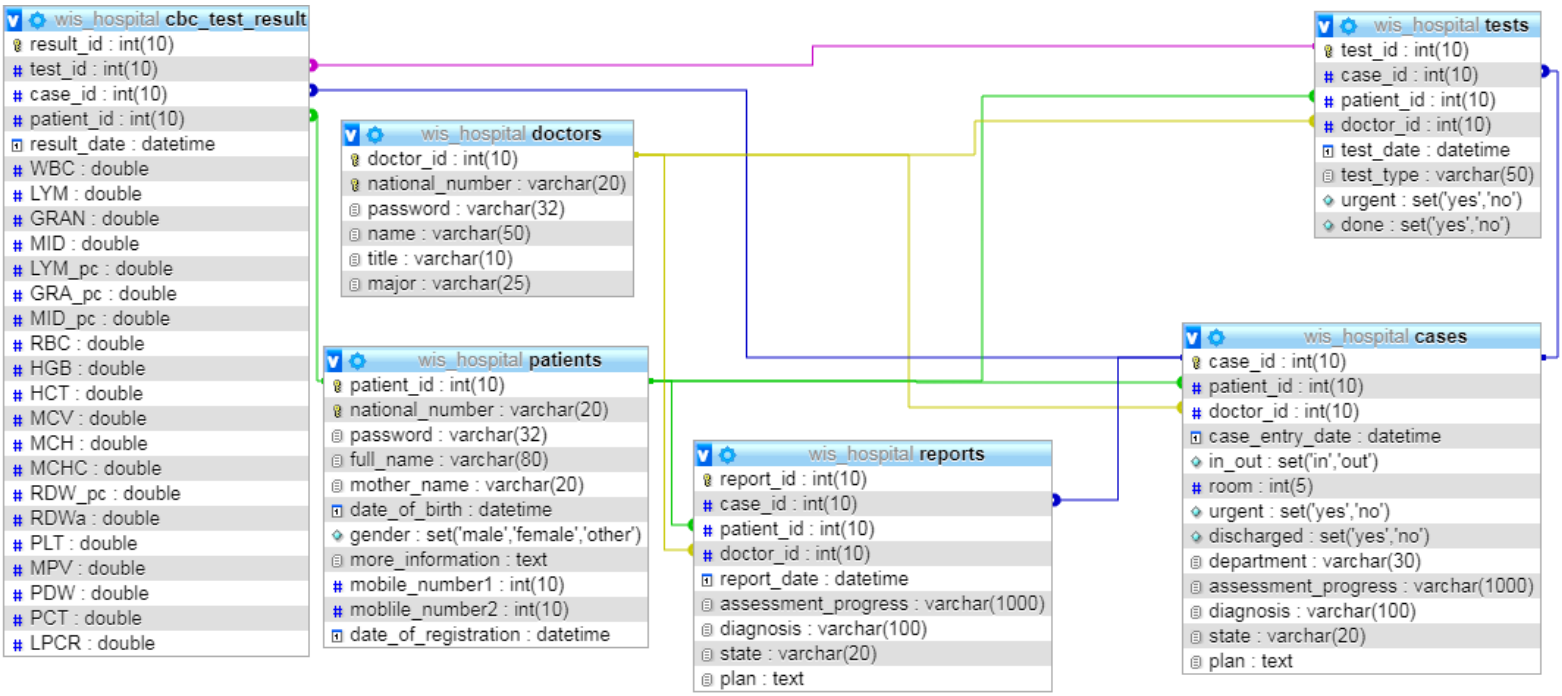
hospitals in Europe or the USA is that in Syria the residents doctor have greater authorities and they are fully responsible in some cases.

- **Application specifications**

In our application we focused in providing a portal for doctors to provide the main health services and to start the process of creating EHRs of patients at the same time. we found that it is important to leave the authority of account creating and patients' registration to a specialized team that should contain both technicians and security staff to check identities and make sure that no patient or doctor is registered more than once. (the website is not fully built, the process of building a comprehensive application is a big process that could take months to present an application that could be launched and then tested and upgraded many times before it could be considered reliable)

As for security we focused on session management and identification check. We chose to open connections with the server inside conditional statements because in the future connections with different authorities should be specified for each type of users. Furthermore, to provide security for passwords, we stored the hashed values of passwords (using MD5 hash).

Here is an image of the structure of our application database and the data for logging in:



Patient account

Name: "ali waseem hassan" password: " patient12123434!!!blabla"

Doctor account

Name: "Waseem Hassan" password: " doctor12123434!!!blabla"

List of References

[1] https://www.healthit.gov/

[2] https://www.ahrq.gov/

[3] https://www.iso.org/

[4] *"ISO 18308:2011 Health Informatics Requirements for an Electronic Health Record Architecture"* National Resource Centre for EHR Standards (NRCeS) Team.

[5] *"Role-based access control through on-demand classification of electronic health record"* Int. J. Electronic Healthcare, Vol. 8, No. 1, 2015.

[6] "Electronic Health Record (EHR)Implementation" Michael Hodgkins, MD, MPH AMA Vice President and Chief Medical Information Officer, Professional Satisfaction and Practice Sustainability, AMA

Tables:

Table -1- Feature values with respect to user role

F	*Feature*	*Doctor*	*Referee Doctor*	*Nurse*	*Relative*	*Insurer*	*Patient*	*Admin*
f_1	Pulse rate	Y	Y	Y	N	Y	Y	N
f_2	Heart rate	Y	Y	Y	N	Y	Y	N
f_3	Temperature	Y	Y	Y	N	Y	Y	N
f_4	SPO_2	Y	Y	Y	N	Y	Y	N
f_4	Blood pressure	Y	Y	Y	N	Y	Y	N
f_5	Blood test	Y	Y	Y	N	Y	Y	N
f_6	Urine test	Y	Y	N	N	Y	Y	N
f_7	Cardiology test	Y	Y	N	N	Y	Y	N
f_8	X-ray	Y	Y	N	N	Y	Y	N
f_9	CT-scan test	Y	Y	N	N	Y	Y	N
f_{10}	HIV test	Y	N	N	N	N	Y	N
f_{11}	Mental test	Y	N	N	N	N	Y	N
f_{12}	Sexual data	Y	N	N	N	N	Y	N
f_{13}	Insurance date	Y	N	N	Y	Y	Y	Y
f_{14}	Insured amount	Y	N	N	Y	Y	Y	Y
f_{15}	Claimed amount	Y	N	N	Y	Y	Y	Y
f_{16}	Insurance type	Y	N	N	Y	Y	Y	Y
f_{17}	Insurance company	Y	N	N	Y	Y	Y	Y
f_{18}	Name	Y	Y	Y	Y	Y	Y	Y
f_{19}	Age	Y	Y	Y	Y	Y	Y	Y
f_{20}	Gender	Y	Y	Y	Y	Y	Y	Y
f_{21}	City	Y	Y	Y	Y	Y	Y	Y
f_{22}	Live status	Y	Y	Y	Y	Y	Y	Y
f_{23}	DOB	Y	Y	Y	Y	Y	Y	Y
f_{24}	Mobile num	Y	Y	Y	Y	Y	Y	Y
f_{25}	Death date	Y	Y	Y	Y	Y	Y	Y
f_{26}	Death reason	Y	Y	Y	Y	Y	Y	Y

Table-2- Problems with Software Functionality and Usability.

Software Quality Domain	Safety Risk	Potential Consequences
Functional Suitability *The degree to which software features are complete, accurate, and appropriate*	Lack of functionality to support clinical workflow	Development of potentially unsafe workarounds
Lack of data coding, standardization, and structure	Lack of appropriate alerts	
Lack of duplicate record detection capability	Fragmentation of information; gaps in documentation	
Inaccurate, incomplete, or outdated decision support rules	High load of false positive alerts; alert fatigue; automation bias resulting in decisions based on incorrect information	
Software bugs	Corruption, loss, or incorrect storage of patient data; incorrect dosage calculations; incorrect linking of orders to medications; potential to introduce new bugs through EHR maintenance and updating processes	
Problematic content import features	Copy-and-paste and other content import features can propagate incorrect, outdated, or improperly attributed information	
Default values	May not be noticed by users and therefore result in incorrect action—e.g., incorrect dosing of medication	
Problematic alerts	Excessive, irrelevant, or low-priority alerts interrupt clinical workflow and can result in distraction; alert fatigue can cause users to miss important alerts	

Simultaneous task performance	Opening multiple records simultaneously can result in documentation errors; editing the same record simultaneously by different users may result in inconsistent information	
Usability *Ease of understanding, learning, and using the interface, including user attraction and accessibility*	Inadequate information displays	Incomplete information display (e.g., medication or allergy information), high information load, and buttons that look alike but have different features can result in patient misidentification or incorrect interpretation of patient data
Unclear current state of user actions in order processing	Clinicians may not be aware of incomplete order submission process; documentation may be incomplete	
Difficult interfaces	Difficult navigation and usability of interface may result in errors in clinical decision making and contribute to errors or delays in treatment	
Error-prone interfaces	Lack of error protection in interfaces—e.g., poor grouping and selection of drop-down menu items—can promote errors, especially in medication ordering	
Efficiency *Processing time, processing capacity, and resource consumption*	Delays in system response	Lack of system responsiveness can result in user inadvertently entering multiple duplicate actions, such as duplicate prescriptions, through repeated clicks
Compatibility *Degree to which 2 or more systems can exchange information*	Intersystem communication errors	Poor interoperability with other systems and failures in network infrastructure can result in delays when patient context or status is not timely or correctly communicated

Reliability *Maturity, availability, fault tolerance, recoverability*	System unavailability	Planned and unplanned EHR downtime can result in lack of access to information