Chapter 1

1. Introduction

Medical Informatics or Health Informatics is the study of resources and methods involved in managing health information. E-health or Electronic health is an emerging field of medical informatics that refers to electronic storage and delivery of health services to the patient. The health domain is adopting IT with a great pace and Hospital Information Systems (HIS) have shown an exponential growth in the last decade. The functionalities of HIS depend on higher heterogeneity of sub-systems built with different specification and protocols. Devices and systems come from different vendors with different network interfaces.

Electronic Health Record (EHR), a by-product of HIS, is segmented through the treatments provided by various care-providers over a period of time. This manifests itself in a variety of forms ranging from general record keeping to specific clinical data for particular areas of care. Ready availability of data improves the quality and delivery of healthcare. Often, it is required to fragment the EHR as per need of the user. The healthcare domain has been slow to adopt IT technologies to manage patient information. Most physicians continue to rely on paper records—leaving room for inefficiencies to share data with other fellow professionals, thus restricting timely and quality care to the patient.

A comprehensive problem list [1] facilitating continuity of care incorporating national standards gives a head start in clinical decision making and quality improvement in interoperable health data exchange. Nations are currently collaborating and taking interoperability initiatives [2] enabling global access of EHR. Enormous research work is undergoing in this domain considering various medical and legal aspects to smooth and secured sharing of health records.

Design effective applications and models to integrate electronically gathered data and knowledge for providing quality care to the patients, is a key to seamlessly share these resources. Moreover, the sensitive health data floats over the network that may increase the probabilities of data being exposed or misused by unauthorized users. Security of confidential health information is another important issue in such environment.
Interoperability enables better workflows, reduced ambiguity, and allows data transfer between disparate EHR systems. Figure 1.1 depicts the stakeholders that share patient’s health records at some point in time. Sharing of EHR occurs not only between inter and intra-hospitals but also with external agencies. It is possible only if all the relevant records of the patient are available in desired format and at required time. To realize their full potential, EHR products must share information seamlessly. Interoperability [3] becomes a constraint due to differences in operating systems, programming language and hardware for those sub-systems. Apart from functional constraints, many other challenges like legal, security and privacy issues, require utmost consideration while designing smooth data transfer from one HIS to another HIS or other relevant parties who may need this information to maintain continuity of care to the patients.

Figure Error! No text of specified style in document..1: Stakeholders of Electronic Health Records

Protecting the medical data and patient’s privacy from all unconcerned is another prime concern. Various methods and techniques prevail for the purpose. Establishing access control, robust encryption techniques and preventing access of data if the device is lost or stolen are a few of them. Timely retrieval of information ensures acceptance and usability of such applications by its prime users. The overall aim is to move health care towards a series of easily available, interconnected, reliable, secured and efficient services. Enormous research work is undergoing in this domain covering all aspects to enable secured sharing of health records. This study focuses on smooth, secured and uninterruptible sharing of health data and proposes a framework for the same.
1.1 Major Security Aspects to EHR Sharing

The outburst of medical data via varied sources opens up number of vulnerabilities to the security and privacy of patient’s data. This demands optimum measures so as to prevent unauthorized access and control in ubiquitous healthcare environment. Following are the general principles that must be properly handled to ensure secured sharing of EHR by health professionals.

1.1.1 Interoperability

Interoperability is the ability of two or more components or systems share and exchange information and resource seamlessly. Information-sharing involves various issues when exchanged in distributed environment. An analysis of various dimensions [4] of interoperable issues; languages, protocols, approaches, standards identifies the challenges pertaining to EHR-exchange. Healthcare interoperability is the sharing of information between medical devices and information systems electronically. Interoperability and deployment of standards for data exchange are technological challenges for which increasingly demanding expectations are being set within the healthcare industry. EHR formats need to be compatible among all providers to maximize the benefits of the technology. Apart from disparate systems, applications, formats, interfaces and vocabularies, many crucial and relevant clauses affect the deployment of interoperable systems in healthcare environment.

1.1.2 Confidentiality

In context with healthcare, confidentiality refers to the disclosure of EHR only to intended and authorized users. Issues and constraints [5] that affect the confidentiality of EHR during storage and transmission over the network need to be identified. Frequent sharing of health records, use of multiple media like CDs, web portals, e-mails or physical copies to transfer records are just few of them. They expose the data to various risks and threats. The CD can be lost, copied or damaged, portals can be hacked, e-mail spoofing is common and data can be stolen. Frequent sharing might result in full access of health details which highly and adversely affects the confidentiality of patient’s identity and health information.

1.1.3 Integrity

Integrity assures that the data is accurate and consistent. Many factors [5] affect the integrity of health records during their use. Poor documentation or typographical errors, use of
shortcut keys, drop-down menus-limiting the choices, are few of them. The contributing factors to integrity loss can be direct or indirect. To understand a direct loss to integrity of EHR let us take two scenarios.

Scenario 1: The patient is discharged from the hospital. The administrative technician generates his discharge report and carries it to the concerned doctor for signature. The doctor edits the report. The technician applies the required editions and gets approval of the doctor. Thereafter, the technician takes the final print, but forgets to save the changes.

Scenario 2: The patient visits OPD. The doctor provides the treatment and prescription to the patient but could not record the observation due to any reason; power failure, delayed response from the system, heavy rush of patients outside or record not available.

1.1.4 Availability

Doctors are on panel of various hospitals or clinics requiring health records of their patients at varied locations. Moreover, there are referral cases where patient’s records are transferred from one hospital to other. The care-providers need to access these records accordingly. The issue of discussion is: How Data should be made accessible to the doctors? Should data be accessed directly from the data store, be available in read-only format or some other robust method needs to be discovered for secured transit of data over the network? Many factors[5] stated below significantly correlate with this issue resulting in poor decision-making:-

Multiplicative extension of access right overtime, access to complete data of the patient, different identification methods for the patients-resulting in inconsistent or duplicate records, disparate access methods, lack of decision-making policies on the amount of data to be transferred, need for monitoring and controlling of the data by IT and hospital staff jointly, effects of stringent security policies, frequency of unavailability of data and augmented chances to data breach due to interoperable sharing of EHRs over the network.

Health Insurance Portability and Accountability Act (HIPAA) [6] enacted as Public Law, specifies “the privacy, security and electronic transaction standards with regard to patient information for all health care providers”. The healthcare professionals need to abide with the code of conduct and follow the guidelines laid by HIPAA to share the EHR with fellow
beings and other related organizations. For instance, as per HIPAA, it is mandatory to take patient’s consent in most of the cases related to the treatment of the patient.

1.2 Rationale of the Study

Designing an environment, where the patient gets all the direct as well as indirect services online, through an integrated and interoperable connectivity of hospitals-private or public, private practitioners, insurance companies, pharmacies and pathological laboratories, demands deep thinking. Most of the hospitals and clinics are in the transition phase of automating health services and maintaining electronic records during patient visits. They have invested a fair amount of money in automation and training of their employees for adapting these healthcare systems. The future demand focuses on availability and accessibility of health records with no restrictions of location and time. This opens up new challenges other than ensuring confidentiality and privacy of health data from malicious intrusion. The hospitals deploy HIS developed on vendor specific architecture, standards and formats. Integration of these varied formats and platforms in a single framework becomes the first task before designing a secured framework for health data availability and accessibility in an open environment across networks. Today’s health IT challenges affects not just providers, but all healthcare stakeholders. Among the challenges that must be addressed are:

- Integrating data from various sources, even those from within the same organization often result in missing, inaccurate, and non-standardized data, thus resulting in data ambiguity.
- Apart from network constraints, ensuring data availability without compromising security entails multiple faults due to disparities in access control rules and policies of healthcare organizations.
- Lack of security measures to protect EHR from misuse or unauthorized access in distributed and unstandardized interoperable environment.

These factors should be carefully and timely dealt so as to prevent irrelevant and undue disclosure of sensitive health records in interoperable sharable environment.

1.3 Objectives

Healthcare demands a strong security of sensitive health records without compromising availability to the legitimate users. Health professionals often need to share these records for
various purposes with multiple agencies. There exists a need to devise a robust security framework that could permit interoperable sharing of EHRs and address the implicit issues in combining EHR-systems of disparate healthcare organizations. This research intends to address and resolve this issue. Hence, the research objectives focus:

- To propose a framework for sharing electronic health records in an interoperable environment.
- To preserve privacy, confidentiality and integrity of health records while integrating with various health-departments.
- To verify the proposed framework using security testing tool.