Current Status of Information Security for Electronic Health Record Services in India

Pulkit Mehndiratta  
Jaypee Institute of Information Technology  
Sector-128 Noida, Uttar Pradesh , India  
pulkit.mehndiratta@jiit.ac.in

Shelly Sachdeva  
Jaypee Institute of Information Technology  
Sector-128 Noida, Uttar Pradesh , India  
shelly.sachdeva@jiit.ac.in

ABSTRACT
With the recent developments in information and communication technology, healthcare is constantly undergoing changes, with new medical technologies, business models and research findings. It has evolved as a new data-centric, more precise, productive, accurate and timely system which can make the difference of life and death in acute situations known as Electronic Health Records (EHRs). The requirements for security and privacy are also very critical and very difficult to satisfy in case of EHRs data as compared to any other data. This is due to the conflicting needs of clinicians (who demand open and easy access to EHRs) and the patients (who prefer closed and private access to EHRs). The potential and capabilities of IT and its influence on the Indian healthcare has been much talked about. Thus, this study examines the current status security and privacy of various EHRs implemented in India. Also, based on the various findings we propose a model to protect the security and privacy of the data subjects (patients).

Categories and Subject Descriptors
H.4 [Information Systems Applications]: Miscellaneous;  
K.6.5.a [Management of Computing and Information Systems]: Security and Privacy

General Terms
Security and Privacy, Electronic Health Records, Inference Control, Developing Country, India

1. INTRODUCTION
Electronic Health Records (EHRs) are the paperless solution to a disconnected healthcare world that runs on a chain of paper files. They provide new opportunities, improves productivity, reduces the administrative burdens, reduce cost and medical errors. These become cavillous in the case of an emergency where the patient may be unable to communicate this information. These provide doctors with more timely access to potentially life-saving information at the point of care while diminishing the paper trail. In general, an EHR includes clinical statements such as observations, laboratory tests, diagnostic imaging reports, treatments, therapies, drugs administered, and allergies. "As more of our medical records are stored electronically, the threats to our security and privacy increase."[1]. Electronic health records form an integral part of the healthcare system and it is imperative that EHR’s are safe because there is evidence that breaches in security have an impact on patients health care. Thus, unless privacy and security problems are resolved, EHRs will not be widely adopted.

2. MOTIVATION
Recent trends in healthcare are adopting standardized EHRs. In developing countries like India, the conventional system of medication is still restricted to paper and pen. EHRs represent lifelike documentation of medical history for any patient. So, an efficient protocol and architecture is required which is not standardized yet [9,10]. Thus, it is utmost important to provide doctors and patients with modern facilities like computer and mobile based medical solution. This will ease the work of practitioners and make it more effective and productive. But, at the same time security and privacy of the data has to be maintained in the system. Few of the security and privacy breaches that occurred in past six to eight months around the globe [4] are due to lack of security and privacy measures and it effected the lives of patients. ISO/TS 18308 standard gives the definition of security and privacy issue for EHRs [2]. According to recent reports, the maximum civil fine for violating Health Insurance Portability and Accountability Act (HIPAA) [3] privacy regulations will increase and become 60 times higher (per provision) from the current $25,000 under an interim final rule published by Health and Human Services in United States. This poster contributes to the current status of EHRs in India and what are the various security and privacy issues. It throws light on, whether various EHRs implemented in India are in compliance with any standard act like HIPAA Act or HITECH Act.

3. METHODOLOGY
In India, apart from C-DAC (Center for Development of Advanced Computing) no other agency is working in the area of Health Informatics and Electronic Health Records (EHRs). C-DAC has developed various solutions such as E-Sushrut [5], DIGHT [6], Mercury, E-Sanjeevi, Tejas, Ayusoft etc. Most of these solutions are indigenously developed and managed by C-DAC only. We have done an extensive study of
Most of the current systems are lacking in the proper security and under development in India. Our findings implicate that ous Electronic Health Records (EHRs) already implemented. We surveyed the problem of security and privacy for various Electronic Health Records Database systems to give maximum security as well as state of the art privacy to the data subjects. This vide security and privacy to the user (data subjects). This project DISHTH (Distributed Infrastructure for Global eHr Technology) [6] proposed to have a separate module for security and privacy which will provide secure storage and access of EHRs, along with privacy to the user. But, till date no such module has been developed/implemented for India to suffice the purpose.

3.1 Proposal for Secure Architecture of EHRs

All the products designed and developed by C-DAC are lacking in security and privacy component in it. Among these, E-Sushrut [5] is the most comprehensive and widely deployed Health Information System. This system incorporates an integrated computerized clinical information system for improved hospital administration and patient health care. The real time version streamlines the flow of patients and simultaneously empowers workflow to perform to their peak ability, but the security and privacy of the patients data is only limited to the user-level access control mechanism. No attention has been paid to the data encryption and anonymity which could lead to inference control. The system also lacks in various measures to protect it from network attacks. Thus, very critical and highly confidential information can easily be compromised due to lack of proper measures.

Project DISHTH (Distributed Infrastructure for Global eHr Technology) [6] proposed to have a separate module for security and privacy which will provide secure storage and access of EHRs, along with privacy to the user. But, till date no such module has been developed/implemented for India to suffice the purpose.

4. RESULTS AND FUTURE SCOPE

We surveyed the problem of security and privacy for various Electronic Health Records (EHRs) already implemented and under development in India. Our findings implicate that most of the current systems are lacking in the proper security and privacy measure for the system and the user information. Some have mentioned to take security and user privacy into consideration are not in compliance with international act or standardized policy set like HIPAA or HITECH Act. Thus, their is a need for imposing very stringent and security policies and procedures. Security issues such as authentication, availability, confidentiality, integrity, access control, data ownership, data protection policies, user profiles and standard model need to be taken into consideration for EHRs. Techniques like k-anonymity [7] and L-diversity [8] should be used to make data more private and anonymous to disable the inferences from the databases. Incorporating security measures and privacy preserving techniques, organizations can benefit from increased user confidence, convenience, and speed of access to information.

A very high level of security and privacy is required for the front-end user application and the back-end database. Thus, in future we will try to come up with an architecture for Standardized EHRs which is in compliance to international standards and protect user privacy and system security.

5. REFERENCES