Issues and Challenges in Securing eHealth Systems

Yan Bai, Institute of Technology, University of Washington Tacoma, Tacoma, WA, US
Lirong Dai, Department of Computer Science and Software Engineering, Seattle University, Seattle, WA, US
Juan Li, Department of Computer Science, North Dakota State University, Fargo, ND, US

ABSTRACT

With the widespread eHealth usage, security of eHealth services is becoming increasingly important. In this paper, we analyze the security problems in eHealth systems, discuss various approaches of securing health data collection and sharing proposed in the recent literature on eHealth security, and provide comparative evaluations that include advantages and limitations of each approach. Possible future research directions on each approach for enhancing security for eHealth applications are also suggested.

Keywords: Access Control, Assisted Living, Cloud Computing, eHealth, Mobile Computing, Pervasive Networks, Privacy, Risk, Security, Sensor Network, Telemedicine, Trust

INTRODUCTION

Electronic health, commonly known as eHealth, delivers and enhances health services and information through the Internet and related technologies [http://en.wikipedia.org/wiki/EHealth]. Examples of eHealth informatics include Consumer Health Informatics, Health Knowledge Management, and Medical Research using eHealth Grids. All these technologies facilitate the provision of general medical information to different users, such as patients, physicians, specialists, care team, pharmacy, and medical researchers. Examples of eHealth services include Electronic Health Records (EHR), Telemedicine, and mHealth:

1. EHR is a collection of electronic health information about individual patients or populations. It includes demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, and billing information. With EHR, health records are available electronically. For healthcare professionals, accessing electronic record is more convenient and flexible than accessing traditional paper-based health records. Moreover, EHR saves cost and space by avoiding multiple copies of a patient’s record at each of his/her doctors’ offices [http://en.wikipedia.org/wiki/Electronic_health_record];
 Telemedicine provides clinical health care remotely that do not require a patient to travel to a specialist [http://en.wikipedia.org/wiki/Telemedicine];

mHealth refers to collect and aggregate patient-level health data, provide healthcare information to practitioners, researchers, and patients, monitor patient vitals, and provide health care service, all using mobile devices. As mobile devices become popular, mHealth will significantly improve the quality of health care [http://en.wikipedia.org/wiki/EHealth].

In summary, eHealth technology improves healthcare quality and significantly reduces the healthcare cost. It gives patients and healthcare professional electronic access to patient records and to health related databases. Medical care could be given remotely to a patient in their home or to a patient in another country. These exciting functions of eHealth do have some issues that need to be further investigated before a more widespread use takes effect. One of the most important issues that must be addressed is security. Specifically, eHealth information system faces a high degree of confidentiality, integrity and availability due to the mass demand of the healthcare services that require an extensive amount of critical, sensitive, and confidential information to be exchanged (Hung, 2007). As explained by Hung et al. (Hung, 2007):

1. **Confidentiality** can be defined as assurance of non-disclosure of sensitive data. It must be maintained to protect the patients’ privacy;
2. **Integrity** can be defined as preventing unauthorized data modification. Integrity must be conserved to ensure that personal health information must not be altered without authorization. Unauthorized change or even loss of personal health information is significantly detrimental because patients’ medical records lead to doctors’ diagnosis and treatment decisions of a patient;
3. **Availability** means that service or data would always be available when it is needed. The availability of eHealth systems is also of great importance because denial of medical service may jeopardize a patient’s personal life.

**Security Threats/Challenges on eHealth**

**Threats to Confidentiality**
Confidentiality attacks occur when electronic access to patient records, to health related databases, to some health-related measurements such as blood pressure, and even to remote diagnosis and treatment are granted without checking the proper credentials. Examples of confidentiality attacks include eavesdropping, location tracking, and activity tracking. Eavesdropping is when an attacker attempts to access medical data while it is acquired, transmitted, or stored either remotely or locally (Kargl, 2008). For example, many eHealth Websites do not use HTTPS, but HTTP protocol (Hong, 2008). When medical information is downloaded from or uploaded to the Websites, it can be easily intercepted by eavesdroppers, because HTTP delivers plaintext, rather than ciphertext. Another example is location tracking in which a person could be tracked as to where he or she currently is and where he or she has been (Kargl, 2008). This is a problem in mHealth systems because messages about a person’s location are constantly sent out, so that the system is able to locate the individual. Lastly, activity tracking, which is unique to eHealth monitoring systems, can be used to determine a user’s daily activities (Kargl, 2008). Confidentiality attacks not only lead to a breach of patient’s privacy but also potentially allow adversaries to modify certain data resulting in wrong diagnosis or treatment.

**Threats to Integrity**
Attacks with which an unauthorized user may modify or intercept medical data cause
Related Content

Levels of Abstraction for Behavior Modeling in the GerHome Project
[www.igi-global.com/article/levels-abstraction-behavior-modeling-gerhome/70006?camid=4v1a](www.igi-global.com/article/levels-abstraction-behavior-modeling-gerhome/70006?camid=4v1a)

Adoption of ICT in an Australian Rural Division of General Practice
[www.igi-global.com/chapter/adoption-ict-australian-rural-division/12918?camid=4v1a](www.igi-global.com/chapter/adoption-ict-australian-rural-division/12918?camid=4v1a)

Privacy and Data Protection towards Elderly Healthcare
[www.igi-global.com/chapter/privacy-data-protection-towards-elderly/77150?camid=4v1a](www.igi-global.com/chapter/privacy-data-protection-towards-elderly/77150?camid=4v1a)
A Systems Framework for Modeling Health Disparities in the Prevalence in Chronic Conditions following a Natural Disaster Event
[www.igi-global.com/article/systems-framework-modeling-health-disparities/77004?camid=4v1a](www.igi-global.com/article/systems-framework-modeling-health-disparities/77004?camid=4v1a)