E-Health Security and Privacy

Yingge Wang
Wayne State University, USA

Qiang Cheng
Wayne State University, USA

Jie Cheng
Wayne State University, USA

INTRODUCTION

The widespread and fast-developing information technologies, especially wireless communications and the Internet, have allowed for the realization of greater automation systems than ever in health-care industries: E-health has become an apparent trend, and having a clinic at home or even anywhere at anytime is no longer a dream.

E-health, including telemedicine featured by conducting health-care transactions over the Internet, has been revolutionizing the well-being of human society. Traditionally, common practices in the health-care industry place tremendous burdens on both patients and health-care providers, with heavy loads of paper-based documents and inefficient communications through mail or phone calls. The transmission of medical data is even messy for cases in which patients have to transfer between different health providers. In addition, the medical documents prepared manually are prone to errors and delays, which may lead to serious consequences. The time, energy, and resources wasted in such processes are intolerable and unimaginable in any fast-paced society. For these problems, e-health provides powerful solutions to share and exchange information over the Internet in a timely, easy, and safe manner (Balas et al., 1997).

Incorporating fast and cost-efficient Internet and wireless communication techniques has enabled the substantial development of e-health. The use of the Internet to transmit sensitive medical data, however, leaves the door open to the threats of information misuse either accidentally or maliciously. Health-care industries need be extremely cautious in handling and delivering electronic patient records using computer networks due to the high vulnerabilities of such information. To this extent, security and privacy issues become two of the biggest concerns in developing e-health infrastructures.

BACKGROUND

As early as 1987, Dr. Thomas Ferguson proposed online health care for consumers. In 1993, Dr. Ferguson, together with several other pioneers, initiated the first national conference on e-health (Nelson & Ball, 2004). The efforts laid the very foundation for the early development of e-health. However, e-health did not make a big step until the late 1990s, mainly due to the technical difficulties and high infrastructure cost. The striking development of information technology, particularly that of the computer, Internet, and wireless communications, dramatizes the reemergence of e-business and e-health (Collen, 1999). Thus, significant improvements to a new health-care infrastructure are anticipated so that health care can take place in a ubiquitous and security-assured manner.

The Internet as a fast, open, and cost-efficient way of exchanging information still faces the big challenge of protecting medical information security and privacy. The information transmitted through the Internet could be accessed, altered, deleted, or copied illegally, jeopardizing the patients' security and privacy. The security issues of e-health, in general, represented by all the precautions taken when safely accessing, collecting, and transferring the health information, must be addressed. In fact, the exchange of health information can be made more secure than in a paper-based system when carefully designed with proper security technologies. Information privacy is controlling whether and how personal data can be gathered, stored, processed, or selectively disseminated (Fischer-Hubner, 2001). Medical information may contain some of the most sensitive information about topics such as one's HIV (human immunodeficiency virus) status, emotional and psychiatric care, and abortions. Thus, the privacy of medical information needs to be especially safeguarded.

Ensuring security and privacy in e-health while preserving the fast transaction of medical data is, however, not an easy task. Security by itself is a complicated and tough task to accomplish in every sense, and there seems to be always a balance between the optimum efficiency and cost vs. maximized security (Fischer-Hubner, 2001). Security in e-business has being studied extensively, yet not a single system has been found to meet the requirements of all levels of protection. Healthcare systems need a higher level of protection because medical data are more sensitive and vulnerable to various misuses or attacks (Mac McMillan, 2002). When accessing medical data, possible errors and attacks could occur during the identification, authentication, and authorization processes. Potential threats and dangers incurred by the transmission of e-health data may come from computer viruses such as Trojan horses and droppers, and from intercepting threats such as masquerading, IP (Internet protocol) spoofing, misrouting, information modifying, and packet sniffing. General security mechanisms, which have been widely used at present, consist of the protection of individual servers and applications, firewalls, and secure data channels during transmission.

An early work conducted by the University of California, San Diego, and others in 1996, titled Patient Centered Access to Secure Systems Online (PCASSO), successfully developed a robust security architecture for Internet access (Baker & Masys, 1999). Since then, more efforts have been directed toward developing e-health security measures for virus protection, firewalls, authentication and access control, encryption, and so forth. Many businesses and research organizations have been developing and marketing their techniques and products, for example, ActiveCard Inc., MediTrust, National Health Key Corroborative, and so forth. Current technologies exploit smart cards, digital signatures, biometric devices, digital watermarking, public-key repository infrastructures, privacy-enhancing techniques, and so on (Ball, Chadwick, & Mundy, 2003; Cheng, Wang, & Tan, 2004). We believe that effective solutions to security and privacy in e-health must rely on a unified framework, with the deployment of wide-range security and privacy technologies from various vendors.

E-health security and privacy are challenging not only due to the difficulties of developing an error-free, complex framework, but also because of the complications of various moral and legal issues among all the stakeholders in the e-health industry such as the consumers, vendors, and health providers. To protect security and privacy in health care, governments around the world need to establish necessary regulatory standards. The Health Insurance Portability and Accountability Act (HIPPA) created in 1996 is a standard made by the U.S. federal government to provide the guidelines and policies that protect medical records. HIPAA presents both challenges and opportunities to improve the way in which medical data are acquired, exchanged, and distributed (Hippaadvisory, 2004). Meeting the challenges of HIPAA legislation requires a careful study of the legal infrastructure and a thorough understanding of the HIPAA evaluation process.

CONCEPTS AND REQUIREMENTS

Security in e-health is an integrated concept requiring the confidentiality, accountability, integrity, and availability of medical data. Confidentiality is ensuring that the data are inaccessible to unauthorized users. Accountability is the ability to trace back all the actions and changes made to the data, for example, through security logs used for recording log-ins, dates, accessed content, and changes. Integrity is preventing information from being modified by unauthorized users. Availability is ensuring the readiness of the information when needed. These four features are equally important and need to be satisfied simultaneously, and by working all together, they encompass the concept of security (Schneier, 2000; Stajano, 2002).

Security issues, in general, cover strategies in four different areas: (a) access security including user-authorization identification and management, (b) communication security related to the secure communication of messages, (c) content security including the protection of content such as data confidentiality, integrity, and availability, and (d) security management including security and vulnerability assessments, the implementation of policies, and guidance (Stajano, 2002; Van de Velde & Degoulet, 2003). To address the above issues, a solution to protecting the privacy and security of e-health needs to accomplish at least the following functions.

- Authentication, the process to validate the identity of the user
- Access control, the process to ensure that only authorized users see the authorized content or information
- Encryption, the process to prevent illegal access or use during data communication
- Intrusion detection and theft termination, the process to automatically detect and disable the devices if they are being accessed or attacked illegally

Privacy is the right of an individual to determine the disclosure and use of this personal data on principle at his or her discretion (Fischer-Hubner, 2001). In e-health applications over the open Internet, privacy may be seriously endangered without sufficient protection by privacy legislation and privacy-enhancing technologies