Chapter 19
E-Health Project Implementation:
Privacy and Security Measures and Policies

Konstantinos Siassiakos
University of Piraeus, Greece

Athina Lazakidou
University of Peloponnese, Greece

ABSTRACT

Privacy includes the right of individuals and organizations to determine for themselves when, how and to what extent information about them is communicated to others. The growing need of managing large amounts of medical data raises important legal and ethical challenges. E-Health systems must be capable of adhering to clearly defined security policies based upon legal requirements, regulations and standards while catering for dynamic healthcare and professional needs. Such security policies, incorporating enterprise level principles of privacy, integrity and availability, coupled with appropriate audit and control processes, must be able to be clearly defined by enterprise management with the understanding that such policy will be reliably and continuously enforced. This chapter addresses the issue of identifying and fulfilling security requirements for critical applications in the e-health domain. In this chapter the authors describe the main privacy and security measures that may be taken by the implementation of e-health projects.

INTRODUCTION

The introduction of technology changed how physicians and other health organizations keep personal health information. In now day's medical data are being kept in a computer, so we talk for an Electronic Patient Record (EPR) and not for a printed medical record. Health information systems rely upon a computerised infrastructure. The development of internet technology and web-based applications made health information more accessible than ever before - from many locations by multiple Health providers and health plans. In the near future, the Internet will probably be the platform of choice for processing health transactions and communicating information and data. But along with this accessibility come increased threats to the security of health information. And those who would steal,

DOI: 10.4018/978-1-60566-768-3.ch019

divert, alter, or misuse personal information are becoming even more skilled at finding what they want and covering their tracks.

PRIVACY AND SECURE INFORMATION EXCHANGE

Health information exchange refers to the sharing of clinical and administrative data across the boundaries of health care institutions and other health data repositories. Electronic information sharing is called electronic health information exchange. Many stakeholder groups (payers, patients, providers, and others) realize that if data could be more readily shared, the safety, quality, and cost of health care processes would improve. From a cultural and technical standpoint, sharing health data is not easy. Stakeholders have competing priorities. Financial concerns, unresolved issues related to rights to access data, and privacy and security issues are among some of the hardest challenges to overcome.

Privacy and security measures are of great concern in all technology sectors, thus leading to ever-evolving, ever-improving protections becoming available. Certainly, public entities must make the most of these developments. In fact, while it is challenging to protect the security of electronic records, it is practically impossible to protect the security of paper records. Electronic records, which can be encrypted and password-protected, are more secure than paper records, less likely to be lost, misfiled, or damaged, and are capable of being backed up. Families must be assured that information provided to the government will only be exchanged with their consent and that, when shared, will be protected from misuse during the transfer.

Medical Data Privacy

Today, individual health and medical data can be collected, collated, stored, analyzed and distributed in unprecedented quantities over the Internet and put to diverse uses for the ease of medical practice. Confidentiality in recording patient information and transferring this information is of utmost importance in protecting patient privacy. These should comply with the Health Insurance Portability and Accountability Act of 1996 protocols protecting patient records. E-health involves new forms of patient-provider interaction, which pose new challenges and threats to privacy issues.

Healthcare is experiencing unprecedented growth in the number and variety of e-health practices being adopted as computer technology and internet network connectivity become increasingly affordable. Data holders operating autonomously, and with limited knowledge, are left with the difficulty of releasing information that does not compromise privacy and confidentiality.

Methodology

There is a set of security services needed for realizing trustworthy e-health solutions. Those security services must be comprehensively integrated in the e-health application. Furthermore, a set of infrastructure services has to be specified and implemented. For keeping the solutions future-proof, they have to comply with architectural principles and paradigms.

The methodology developed is based on 3 key assumptions. The first assumption is that, in order for stakeholders to trust electronic health information exchange, decisions about how to protect the privacy and security of health information should be made at the local community level. Second, to accomplish this goal, discussions must take place to develop an understanding of the current landscape and the variation that exists between organizations within each state and, ultimately, across states. Finally, stakeholders at the state and community levels, including patients and consumers, must be involved in identifying the current variation, understanding the rationale that

Insight into Disrupted Spatial Patterns of Human Connectome in Alzheimer's Disease via Subgraph Mining
Junming Shao, Qinli Yang, Afra Wohlschlägerand Christian Sorg (2012). *International Journal of Knowledge Discovery in Bioinformatics (pp. 23-38).*
www.irma-international.org/article/insight-into-disrupted-spatial-patterns/74693