Chapter 10
Safety and Security in Professional and Non-Professional E-Health and Their Impact on the Quality of Health Care

Suzana Parente
Portuguese Association for Quality in Health Care, Portugal

Rui Loureiro
Portuguese Association for Quality in Health Care, Portugal

ABSTRACT

E-health involves professionals and non-professionals and raises safety and security issues that affect the quality of health care. Therefore, the chapter provides some basic ideas on e-health safety and security, focusing on the healthcare provider perspective. To clarify some of the controversies and some of the problems in the use of data, arising from the use of e-health without taking into consideration the safety and security issues, we present one novel unpublished case and six cases from the Food and Drug Administration (FDA), Multi-Media Consumer Information, (FDA) Patient Safety News. Topics highlight fraud, impersonation of health care professionals, misuse of data and information, and backups.

INTRODUCTION

E-health is prevalent. It covers everything from patient to professional identification, prescribing, clinical data, accounting to management of medical devices, pharmaceuticals and safety and security of healthcare facilities (e.g. fire, intrusion, flooding). Moreover, the Internet is a key component in every facet of today's life, including even older users (the fastest growing group of Internet users). As a result, it has an impact on the implementation of IT in healthcare, especially regarding the non-professional users of e-health. Furthermore, the development of the Internet from the web 1.0 to 2.0 to the semantic web will undoubtedly play a vital role in the application and misuse of e-health (Goodenough, 2009).

DOI: 10.4018/978-1-61692-843-8.ch010

Social networks like today's Facebook, Twitter, blogs and chat rooms, should also be analyzed for their impact especially in the non-professional e-health sector.

Overall, there are two types of clients in e-health, which include the professional user, healthcare professionals of all specialties, and the non-professional user, who acts as a supplier of data and end user. Consequently, we might distinguish two dimensions e-health, which affect the health care options of a growing number of individuals in modern societies.

1. Professional e-health, which encompasses the use of IT by healthcare professionals and patients.
2. Non-professional e-health, which includes Internet data on diseases, procedures, medical devices, and pharmaceuticals.

On the other hand, ensuring the privacy and confidentiality is an indispensable component of health information systems (Doupi et al., 2005) while safety and security, the most salient issues when quality in e-health is concerned, are not the task of IT specialists. It is also the responsibility of healthcare organizations and healthcare providers (Katsikas et al., 2008).

The evolution from an organization-centered to a process-related and to a person-centered health system involves many aspects of security, safety, privacy, ethics, and quality (Blobel, 2007). Therefore, while discussing about health information systems, we need to implement new technologies in order to face challenges arising from both legal and technological background (Blobel, 2007; Pharow, P. & Blobel. 2009). The lessons learned in the last years clearly show that e-health is more than just a straightforward change from paper records to electronic records. It calls for a paradigm shift and the use of new technologies and procedures (Hildebrand et al., 2006). As a result, interoperability, security and confidentiality are vital for the acceptance of the new approaches, the quality improvement, and the safety of patient's care (Hammond, 2008; Engel et al., 2006). Safety is the cornerstone of quality and an integral consideration in all aspects of care delivery (IOM, 2001).

On clinical grounds, the growing availability of solutions, which monitor remote health-related data, using wireless networks technologies (e.g. ECG, blood pressure monitoring, lab tests) reinforces the e-health importance. Events like the severe acute respiratory syndrome (SARS) and the swine flu pandemic provide excellent case studies of the overall impact of IT on health care. However, reliable information (public or/and professional) coexists with rumors, misleading information, counterfeit medicines, counterfeit medical devices and diagnostic tests.

Finally, it is worthwhile mentioning that IT safety and security involve professionals and non-professionals, and deal with issues like (Adibi, et al., 2008; De Meyer et al., 2008; Savastano et al., 2008):

- hardware security
- password protection of received/sent files
- encryption of communication data
- encryption of stored data (e.g. files, e-mails, data files, image files, audio files)
- e-signatures
- safety copies of stored data(backups)
- software validation
- software license hardware accesses
- software accesses
- redundant processing

However, the chapter will outline the basics of e-health safety and security emphasizing on the provider perspective.

BACKGROUND

E-health is a new word and concept, which arises at the end of the 20th century (Eysenbach, 2001;