briefing paper

digital preservation europe

Security aspects in electronic personal health record: data access and preservation

The world of applied medical informatics is changing rapidly due to an increasing use of the results of Information Systems reports, data trending and images. Recent advances in Information and Communication Technology (ICT) give access to patients with chronic conditions at home through particular e-Health services such as Telemedicine. The development of online services such as "teleconsultation, e-prescription, e-referral, telemonitoring and telecare" has created new, remote health care functions that potentially threaten privacy. Indeed, confidentiality concerns remain a sensitive point of discussion in the digital age. This article describes which measures can be implemented to strengthen personal data security.

Introduction

Information communication technology (ICT) has had a dramatic impact on our daily lives in recent years, benefiting many areas of the public health including health care delivery, surveillance, research and education. ICT provides more convenient ways to accomplish daily tasks and diminishes the impact of long distances in both personal and business interactions. Interaction between patients and physicians through the use of electronic tools for health-related purposes has been broadly defined as "e-Health" [1-3].

E-Health activities are becoming quite common in our society and using the latest ICT have the potential to transform the health care delivery systems both in advanced and emerging nations by meeting the needs of citizens, patients, healthcare professionals, providers, and policy makers [1-9]. It is recognised that the achievement of the benefits from e-Health are dependent on a secure, robust and reliable organisational and technical framework to enable continuity of healthcare [1-3]. A Global Observatory for e-Health dedicated to understanding the e-Health domain, its growth, evolution, and impact on health systems in all countries has been developed by the World Health organisation [WHO, 9]. Moreover, the European Community considers as a priority action "initiative on telemedicine (TM) for chronic disease management as home health monitoring" and the future "vision for Europe 2020" is based on development of "integrated Telemedicine Services" [10,11].

TM is defined as "medicine practiced at a distance". It combines the expertise of a professional clinical staff, medical equipment, computer hardware, software and communication technology, through a service centre, to examine, investigate, monitor and treat patients in distant places [3,12]. In 2001 TM opportunities were summarized as: 1) Home Telenursing, 2) Electronic referrals to specialists and hospitals, 3) Teleconsulting between General Practitioners (GPs) and specialists, 4) Call centres' activities and online health.

The present article will develop aspects related to security in the management of electronic personal referral through a TM service.

What is an Electronic Personal Health record?

Although no universally accepted definition exists, EPH can be described as "an electronic application through which individuals access, manage and share their health information… in a private, secure and confidential environment". Models vary in the extent to which the content of the records and rights of access are controlled by the patient (simple models) or the healthcare provider (complex models), the range of tools used (i.e. telephone, electro-medical devices, Videophone, computers, wireless and internet technologies) and their interactivity. TM can be considered a complex system including integrated information such as medical history, results from examinations, images and documents for which authorized access by the health care team members has to be considered.

EPH pros

Due to the promise of improved quality and efficiency through better maintenance and availability of personal patient data the potential of EPH record is considerable. It offers many advantages over paper records since information can be more standardized, permitting faster retrieval and review. Incompatibility between different databases and systems can be diminished with the adoption of consistent technology and standard data whilst effective management between GP and patient to record historical data could also be improved. EPH empowers patients and clinicians to share decision-making and clinical outcomes, reducing geographical barriers and improving continuity of care and efficiency especially for the chronically ill.

What are the key strategies for handling sensitive information?

There is an emerging literature about the legal aspects of TM and Electronic Health Record (EHR) technologies. As a preventive measure TM should refer to two main points: education and preventive engineering.

Education:

Special training around issues of confidentiality is an integral part of prevention. To realise their potential, EHP records integrated within TM care processes need educational initiatives to achieve greater vigilance in handling documents and devices by fully professional staff who are sensitive in the use of clinical terms and educated in the values of internet hygiene and security issues.

Preventive engineering:

Security, integrity and privacy of personal medical data is of utmost importance, and whilst many research projects worldwide are investigating the application of new technologies to pervasive healthcare solutions, security and reliability of these technologies is an area that requires further exploration. In the last years a number of bodies and working groups have been developing standards and guidelines specifically for medical data transmission and preservation. Perhaps the most useful standards that are currently available are those relating to the generation and use of EHR, most of which have been in development since national organisations in Europe and the UK began the process of electronic conversion of the population's health records. DICOM (Digital Imaging and Communications in Medicine) and Health Level 7 Communication Standard (HL7) are just two examples of standards that have been growing up in the last years. In essence, the main characteristics that a Healthcare network security system should provide are:

a. User authentication to verify requests for access to data
b. User authorisation to permit access to data
c. Ensured confidentiality of data transmitted over the communications network.
d. Integrity of data

Authentication is the process that verifies the identity of people that access personal medical data contained in the EHR. The process is initiated on the input of the system user's identity and is completed when the identity is recognized. The system takes into account identities based on one or more factors that the user knows (for example a password) or owns (for example a smart card).

Authorisation is a process in which the system protects resources by only allowing them to be used by authorised resource consumers. Regarding EHRs, usually patients themselves give authorisation to some figures to access their data (GPs, nurses, etc.).

Confidentiality means that the data contained in the EHRs shouldn't be intercepted during its transmission and used by unauthorized people. This is the most important requirement that systems which handle EHRs must satisfy. Patients' personal and health information has to be encrypted to avoid unauthorized access.

Integrity means that data in the EHR cannot be created or amended without the right authorization. Integrity involves both users and systems.

Following these main requirements, different solutions have been implemented. However a standardized approach to the development of EHRs is still lacking. The biggest problem in health care is the challenge of data availability. There are over 700 standards in health care. These standards are intended to synchronize health care entities with the rest of the world. However, it has been debated that today's standards will be almost obsolete in 5 years. Several models of standardization for electronic medical records and electronic medical record exchange have been proposed and multiple organizations have been formed to help evaluate and implement them. However, the idea that patients' privacy has to be protected is universal. As the ever-changing healthcare industry evolves, one key topic within the EHR is privacy. Both in the USA and in the EU, several directives protect the processing and free movement of personal data, for purposes of health care, and set guidelines that all healthcare organizations will have to comply with in regards to electronic health transactions.

Further information and resources

1.Wootton R. Telemedicine: Clinical review. BMJ 2001; 323: 557-60.

2.Home telehealth: connecting care within the Community". Edited by R. Wooton S. L. Dimmick JC Kvedar. The Royal Society Medicine Press Ltd London, april 2006.

3.Scalvini S, Vitacca M, Paletta L, Giordano A, Balbi B. "Telemedicine : a new frontier for effective healthcare services" Monaldi Arch Chest Disease 2004;61:4,226-233.

4.Mair F, Whitten P. Systematic review of studies of patients satisfaction with telemedicine. BMJ 2000; 320:1517-1520.

5.American College of Physicians. E-Health and Its Impact on Medical Practice. Philadelphia: American College of Physicians; 2008: Position Paper. (Available from American College of Physicians, 190 N. Independence Mall West, Philadelphia, PA 19106.)

6.Barlow J, Singh D, Bayer S, Curry R. A systematic review of the benefits of home telecare for frail elderly people and those with long-term conditions. J Telemed Telecare. 2007; 13(4):172-9.

7.Clark Ra, Inglis SC, McAlister FA et al. Telemonitoring or structured telephone support programmes for patients with chronic heart failure: systematic review and meta-analysis. BMJ 2007;334(7600):942.

8.Paré G, Jaana M, Sicotte C. Systematic review of home telemonitoring for chronic diseases: the evidence base. J Am Med Inform Assoc. 2007 May-Jun; 14 (3):269-77.

9.Meystre S. The current state of telemonitoring: a comment on the literature. Telemed J E Health. 2005 Feb; 11 (1):63-9.

10.Young HM. Challenges and solutions for care of frail older adults. Online J Issues Nurs. 2003; 8 (2):5. World Health Organization Global Observatory for eHealth. Global eHealth Survey Geneva July 2005

11.EHTEL. Sustainable Telemedicine: paradigms for future –proof healthcare. A briefing paper 20 february 2008

12.Ministers of EU Member States Ministerial Declaration. eHealth. Brussels, 22nd May 2003

Authors: Laura Comini, Marco Mazzu', Simonetta Scalvini,
Fondazione Salvatore Maugeri IRCCS, Servizio Autonomo di Telemedicina, Lumezzane (BS) Italy
simonetta.scalvini@fsm.it