

Chapter 62

Implementation Issues on a National Electronic Health Record Network

John McGaha
Capella University, USA

ABSTRACT

The United States congress and the past several administrations have dedicated considerable funding for incentives focused on accelerating the adoption by the healthcare industry of Health Information Technology (HIT) solutions. The most recent effort towards these objectives includes a focus on the creation of a National Health Information Network that will support large scale exchange of health information. This chapter explores the technical, security and privacy implications of the advent of such an integrated network and the steps towards its successful completion.

INTRODUCTION

An electronic health record (EHR) contains a patient's medical history in electronic format. Access to an EHR with Internet technologies has the potential for early detection and response to bioterrorist attacks; nation-wide and global monitoring and treatment of communicable disease; and monitoring, detecting, and treating exposures to biochemical agents (Teich, Wagner, Mackenzie, & Schafer, 2002).

Information security is vital to the operation, success, and sustainability of today's information-centric organizations, such as those in the health-care business, and is now a top business concern on a global scale (Filipek, 2007). There are many obstacles preventing the implementation of a national electronic health record (EHR) infrastructure. This project examines the issues stakeholders have with the adoption of an EHR network and identifies some effective measures that can be taken to minimize the security risks inherent to sensitive information shared across a national network. Common obstacles at the lo-

DOI: 10.4018/978-1-4666-2770-3.ch062

cal and national level include funding, privacy, security and accuracy of sensitive data. Common obstacles on a global level include communication, standardization, funding and interoperability (Arnold et al., 2007).

BACKGROUND OF REGULATORY CONTROLS IN HEALTH CARE

In an information system, controls are actions taken by people or software to minimize security risks. Controls also serve to direct desirable behavior and processes in an organization (Carter, Cobb, Earhart, & Noblett, 2008). The healthcare and financial industries are compelled to comply with several government imposed regulations (controls). While many organizations have developed and implemented their own sets of controls, the federal government enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996. The Act requires security and privacy controls on managing medical data. Organizations are required to comply to HIPAA regulations if the organization provides a health plan for employees, provides healthcare to patients, or provides healthcare insurance. Compliance to HIPAA is enforced by the US Health and Human Services (HHS) Department. The law requires the HHS to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers (HISPC, 2007).

Failure to properly apply HIPAA security controls can result in civil monetary penalties imposed by the HHS. The Security of Treasury is empowered to impose tax penalties on organizations that are not in compliance (Foulitz, 2004). After February 18, 2010, the HHS is authorized to penalize HIPAA violators up to \$1.5 million, a 60% increase of current limits (CMIO, 2009). This new authorization is problematic because many healthcare providers are not in compliance with HIPAA primarily due to the lack of funds

and understanding the regulations (Netchert, 2008; Foulitz, 2004).

In 2004, President Bush directed the HHS to develop, plan, and guide the implementation of nation-wide health information technology (GAO-07-988T, 2007). As part of the directive, the HHS is responsible for the protection of personal health information that will populate a nation-wide healthcare database. The GAO report identifies key challenges that have yet to be addressed by the HHS. Challenges associated with the safeguarding the exchange of electronic health information include: understanding and resolving legal and policy issues; ensuring appropriate disclosure; ensuring individual's rights to request access and amendments to health information; and implementing adequate security measures for protecting health information.

The Health IT for Economic and Clinical Health (HITECH) Act enacted in 2009 gives the HHS authority to impose increased financial penalties on organizations in non-compliance to HIPAA. Maximum fines outlined in HIPAA are a maximum of \$25,000. According to HITECH regulations, the HHS can fine organizations up to \$1.5 million (HHS, 2009) for HIPAA violations. The Health Information Technology for Economic and Clinical Health (HITECH) Act is part of the contested stimulus legislation. HITECH authorizes limited funding of EHR implementation.

HEALTH INFORMATION EXCHANGE

A prelude to a national EHR network (and global network) is the Health Information Exchange (HIE). At least 35 states are actively involved with creating state-wide electronic medical record systems that will exchange health information (Dimitropoulos & Rizk, 2009). The technical architecture of a national health information exchange (HIE) is yet to be developed. However, in early 2010, the federal government will begin distributing \$564 million to states to fund state-level HIE

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/implementation-issues-national-electronic-health/73888

Related Content

Bring Your Own Device in Healthcare

Ailton Moreira, Carlos Filipe da Silva Portela and Manuel Filipe Santos (2019). *International Journal of Privacy and Health Information Management* (pp. 1-13).

www.irma-international.org/article/bring-your-own-device-in-healthcare/267201

A Transaction Cost Assessment of a Pervasive Technology Solution for Gestational Diabetes

Nilmini Wickramasinghe, Indrit Troshani, Sally Rao Hill, William Hague and Steve Goldberg (2013). *Healthcare Information Technology Innovation and Sustainability: Frontiers and Adoption* (pp. 109-126).

www.irma-international.org/chapter/transaction-cost-assessment-pervasive-technology/73817

Real-Time, Location-Based Patient-Device Association Management: Design and Proof of Concept

Raoufeh Rezaee, Malak Baslyman, Daniel Amyot, Alain Mouttham, Rana Chrey and Glen Geiger (2017). *International Journal of Healthcare Information Systems and Informatics* (pp. 37-61).

www.irma-international.org/article/real-time-location-based-patient-device-association-management/182481

Telehealth-Based Systems for Diagnosis, Management, and Treatment of Autism Spectrum Disorders: Challenges, Opportunities, and Applications

Fiorentina Angjellari-Dajci, William F. Lawless, Nitin Agarwal, Ron Oberleitner, Barbara Coleman and Masoud Kavoossi (2013). *Handbook of Research on ICTs and Management Systems for Improving Efficiency in Healthcare and Social Care* (pp. 1044-1065).

www.irma-international.org/chapter/telehealth-based-systems-diagnosis-management/78069

Sentiment Analysis for Health Care

Muhammad Taimoor Khan and Shehzad Khalid (2015). *International Journal of Privacy and Health Information Management* (pp. 78-91).

www.irma-international.org/article/sentiment-analysis-for-health-care/142225