Patient Centric Healthcare Information Systems in the U.S.

Nilmini Wickramasinghe
Illinois Institute of Technology, USA

INTRODUCTION

Healthcare expenditure is increasing exponentially, and reducing this expenditure (i.e., offering effective and efficient quality healthcare treatment) is becoming a priority not only in the United States, but also globally (Bush, 2004; Oslo Declaration, 2003;Global Medical Forum, 2005). In the final report compiled by the Committee on the Quality of Healthcare in America (Institute of Medicine, 2001), it was noted that improving patient care is integrally linked to providing high quality healthcare. Furthermore, in order to achieve high quality healthcare, the committee has identified six key aims, that is, healthcare should be:

1. **Safe:** avoiding injuries to patients from the care that is intended to help them
2. **Effective:** providing services based on scientific knowledge to all who could benefit, and refraining from providing services to those who will not benefit (i.e., avoiding under use and overuse)
3. **Patient centered:** providing care that is respectful of and responsive to individual patient preferences, needs, and values, and ensuring that patient values guide all clinical decisions
4. **Timely:** reducing waiting and sometimes harmful delays for both those receiving care and those who give care
5. **Efficient:** avoiding waste
6. **Equitable:** providing care that does not vary in quality based on personal characteristics

Most of the poor quality connected with healthcare—such as loss of information or incomplete information pertaining to patient medical records, allergic reactions that can be life threatening, or the ordering of wrong tests—is related to a highly fragmented delivery system that lacks even rudimentary clinical information capabilities resulting in inadequate information flows and poorly designed care processes characterized by unnecessary duplication of services, long waiting times, and delays (Institute of Medicine, 2001; Chandra, Knickrehm, & Miller, 1995). In addition, poor information quality is also a major contributor to the numerous medical errors that permeate throughout the system (Mandke, Bariff, & Nayar, 2003). The introduction of the Health Insurance Portability and Accountability Act (HIPAA, 2001) in the United States into this context only makes matters more complex, since it imposes a further level of convolution to the design and management of information and its flows throughout the healthcare system. The aims of HIPAA are indeed laudable, since they focus on establishing better governance structures and compliance so that healthcare information can be protected and secured; however, in practice, given the current platform-centric nature of healthcare organizations, this only serves to create further informational challenges.

Healthcare is noted for using leading-edge technologies and embracing new scientific discoveries to enable better cures for diseases and better means to enable early detection of most life-threatening diseases (Stegwee & Spil, 2001; McGee, 1997; Johns, 1997; Wallace, 1997). However, the healthcare industry has been extremely slow to adopt and then maximize the full potential of technologies that focus on better practice management and administrative needs (Stegwee & Spil, 2001). In the current complex healthcare environment, the development and application of sophisticated patient-centric healthcare systems and e-health initiatives are becoming strategic necessities, yet healthcare delivery has been relatively untouched by the revolution of information technology (Institute of Medicine, 2001; Wickramasinghe, 2000; Wickramasinghe & Mills, 2001; Stegwee & Spil, 2001; Wickramasinghe & Silvers, 2002). To address this dilemma, healthcare organizations globally require a systematic methodology to guide the design and management of their respective IC^2T adoptions, not only to be compliant with regulations like HIPAA but also to be able to capture, generate, and disseminate information that is of high integrity and quality, and thereby be both technically sound and

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

meet the highest ethical and security standards. An integrative compliance framework is an appropriate solution strategy.

REGULATORY REQUIREMENTS

In the United States, HIPAA (2001) is the minimum governing regulatory compliance standard to which healthcare organizations must adhere. Essentially similar standards exist in other countries, for example, the EU Directive 46 of 1995 is currently being implemented throughout all EU countries, as well as revisions to this, including privacy law (675/96) (Inchingolo, 2003). These are developed by countries or respective governments within the EU to ensure security and privacy of sensitive patient healthcare information. Irrespective of which policy we look at (HIPAA or the EU Directive), the fundamental areas pertaining to compliance and security of health information are similar. A closer examination of HIPAA reveals three key elements: security, privacy, and standards for electronic submissions and exchange of healthcare information (HIPPA, 2001; Moore & Wesson, 2002).

Security

According to HIPAA, a number of security criteria must be met, not only by the housing of information but also by all electronic healthcare transactions that contain healthcare information. Some of these criteria directly affect how healthcare systems can be accessed as well as how the key healthcare players (governments, providers, payers, and patients) may interact with these systems. The HIPAA security requirements[1] focus on:

- establishing trust partnership agreements with all business partners
- instituting formal mechanisms for accessing electronic health records
- establishing procedures and policies to control access of information
- maintaining records of authorizing access to the system
- assuring that system users receive security awareness training, and the training procedures are periodically reviewed and updated
- maintaining security configuration including complete documentation of security plans and procedures, security incident reporting procedures, and incident recovery procedures;
- ensuring communication and network control, including maintaining message integrity, authenticity, and privacy; encryption of messages is also advocated for the open network transmission portion of the message; and
- authenticating data to ensure it is not altered or destroyed in an unauthorized manner.

The principal security tenets of HIPAA fall into three categories—administrative, physical, and technical—each subdivided into several sub-categories consisting of multiple levers (Wickramasinghe & Fadlalla, 2004). Table 1 summarizes the major issues and levels under each of these categories.

Transaction Standards

The standards for electronic health information transactions cover all major transactions, including claims, enrollment, eligibility, payment, and coordination of benefits. HIPAA discusses two major categories with relation to transaction standards: practice standards and technical standards. The key practice standards are:

1. Health Care Common Procedure Coding System (HCPCS)
2. ICD-9–Diagnosis Codes
3. ICD-9–Procedure Codes

The technical standards focus on the adoption of electronic data interchange (EDI) using health care industry implementation guidelines and other standards such as XML and X12. Plans and providers can comply with these standards directly or via a healthcare clearinghouse (Wickramasinghe & Fadlalla, 2004).

Privacy

The final element of HIPAA focuses on ensuring the privacy of healthcare information. Patient healthcare data is sensitive in nature and must be protected from the potential and possibility of misuse or abuse. Specifically, the *Federal Register* (vol. 67, no. 157) details all the rules that must be adhered to with respect to privacy. The purpose of these rules is to maintain strong protection for the privacy of individually identifiable health information. Thus, these privacy requirements

7 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/patient-centric-healthcare-informationsystems/13517

Related Content

Subjective Attack Trees: Security Risk Modeling Under Second-Order Uncertainty
Nasser Al-Hadhrami (2023). *International Journal of Blockchain Applications and Secure Computing (pp. 1-27).*
www.irma-international.org/article/subjective-attack-trees/320498

An Improvised Framework for Privacy Preservation in IoT
Muzzammil Hussainand Neha Kaliya (2018). *International Journal of Information Security and Privacy (pp. 46-63).*
www.irma-international.org/article/an-improvised-framework-for-privacy-preservation-in-iot/201510

Cyber Resilience for the Internet of Things
Marcus Tanqueand Harry J. Foxwell (2018). *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution (pp. 304-335).*
www.irma-international.org/chapter/cyber-resilience-for-the-internet-of-things/206788

An Analysis of Economic Growth for Major Advanced Economies
Hakan Altin (2022). *International Journal of Risk and Contingency Management (pp. 1-22).*
www.irma-international.org/article/an-analysis-of-economic-growth-for-major-advanced-economies/295958

Enhancing Intrusion Detection Systems Using Intelligent False Alarm Filter: Selecting the Best Machine Learning Algorithm
Yuxin Mengand Lam-For Kwok (2014). *Architectures and Protocols for Secure Information Technology Infrastructures (pp. 214-236).*
www.irma-international.org/chapter/enhancing-intrusion-detection-systems-using-intelligent-false-alarm-filter/78873