Chapter 5.4
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 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 requirements1 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