ABSTRACT

This article presents the design and architecture of a health information system that takes into account various requirements posed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The recommendations made, primarily address Health Care Provider and Health Plans’ needs. It introduces the reader to common HIPAA terminology, then picks a specific enterprise technology stack, i.e. Java Enterprise Edition (J2EE) and delves into some of its relevant artifacts. The article makes recommendations for tools, techniques and design guidelines to facilitate the architecture of a HIPAA compatible information system. We focus primarily on Health-care Providers and a subset of Health Plans. These entities have one thing in common: they process or store health information, hence they fall under HIPAA’s purview. The architecture model that we are proposing will attempt to present a unified security model (e.g. security in client, application and database layers).

Keywords: HIPAA; information security; java applet; J2EE; software architecture

INTRODUCTION

The health care industry is one of the largest and most critical components of modern economies. Health care spending accounts are approximately 12% of Canadian and 16% of American gross national product (GNP) (Chiasson & Davidson, 2002). In fact, health care spending is rapidly escalating, resulting in a growing concern to consumers, policy makers, and business managers. Information technology (IT) applications such as computer-based patient records, clinical information systems, and telemedicine have the potential to greatly improve cost effectiveness, quality, and accessibility of health care. Although IT uses in health care settings have lagged behind IT use in other industries (Menon & Lee, 2000), significant increases in IT spending in many health care organizations in recent years, combined with interest and an active pursuit of “e-commerce” (sometimes called “e-health”) initiatives, have generated immense interest in health information systems among organizational strategists, government regulators, and citizen groups. Their interests and concerns range from economic impacts of IT spending on industry cost structure, to the implications of IT use for health care quality, and to patient privacy protection in the age of electronic health care systems.
A major challenge that patients face in health care today is the lack of access to their complete health information. Ideally, patients shall have a comprehensive and updated version of their health information, which can also be made available to any provider that they wish to see. As individuals move, travel, switch health insurance carriers, and get their care from different providers, their medical records are distributed across multiple sites where they have received care. These records generally cannot be exchanged and updated unless the sites are part of a network of providers that share common information systems (Department of Health and Human Service, 2005). Past medical records are an important input in clinical decision making and without the consolidation of all relevant medical information, there is a substantial risk of medical errors, delays in diagnosis, and inefficient treatment. The personal health record (PHR), a Web-based patient owned electronic medical record (EMR) (Shortlife, 1999), was created to consolidate all of a patient’s medical information in a single, yet secure, location. PHR systems developed in the late 1990s were targeted for patients who were traveling and needed health care, or in emergencies where patients were unconscious and unable to provide their health information. Typical information in these PHRs included patients’ medical histories, insurance information, allergies, immunizations, medications, and past surgeries. Many studies have been conducted to evaluate PHRs on criteria for provider-owned EMRs, comparing features and examining the user interface (Kim & Johnson, 2002; Schneider, 2001; Wang, Lau, Matsen & Kim, 2004). Common features in EMRs, such as using International Classification of Diseases codes to precisely identify diseases, could not be implemented easily in PHRs, where patients are responsible for data entry. The reliability of patient-entered data has also been questioned.

Health information represents one of the most sensitive types of information to be processed and stored by an organization. The concern for privacy and security needs of the patients is so serious that the government has had to introduce legislation in order to regulate the use and maintenance of this information by organizations. Any negligence on the organization’s part can result in heavy penalties and enormous loss of goodwill in public. In the United States the confidentiality of health information has historically been governed by different standards administered by various federal, state, and local statutes, regulations, and case law. These disparate and fragmented directives were part of the an effort for the creation of uniform standards through the application of federal law, such as the Health Insurance Portability and Accountability Act of 1996, known as HIPAA. It also mandates major paperwork reduction and data standardization practices in patient record documentation (Lanser, 2001; Public Law, 1996). In addition, the Federal Medical Privacy Rule (MPR) came into effect on April 14th, 2003 (Schneider, 2001). HIPAA (Public Law, 1996) gives patients greater access to their own medical records and more control over how their protected health information (PHI) is used. The regulation also addresses the obligations of health care providers and health plans (including Medicare and State Medicaid programs) to protect health information. In general, covered entities such as health plans, health care clearinghouses, and health care providers (which conduct certain financial and administrative transactions electronically) had until April 14, 2003, to comply. Since privacy and security in the context of HIPAA are invariably interconnected; any text on HIPAA will focus heavily on security guidelines to ensure that the individuals’ rights to privacy of their health care data are not violated. IT managers who deal with health information management systems have to stay abreast of HIPAA guidelines. To ensure compliance of legacy systems that have little or no built-in support for these guidelines is a daunting task and cannot be addressed in a generic fashion.

**HIPAA**

This section covers some of the abstractions identified in the HIPAA Act that will serve as a basis to develop our generic health information systems.
Related Content

Inventing the Future of E-Health
www.igi-global.com/chapter/inventing-future-health/49851?camid=4v1a

Developing Smart Emergency Applications with Multi-Agent Systems
Federico Bergenti and Agostino Poggi (2010). International Journal of E-Health and Medical Communications (pp. 1-13).
www.igi-global.com/article/developing-smart-emergency-applications-multi/47534?camid=4v1a

Regularity Analysis of the Magnetoencephalogram Background Activity in Alzheimer's Disease Patients Using Auto Mutual Information
www.igi-global.com/chapter/regularity-analysis-magnetoencephalogram-background-activity/13057?camid=4v1a
The Effects of Electronic Medical Record (EMR) Use in Primary Care on the Physician-Patient Relationship


[www.igi-global.com/chapter/effects-electronic-medical-record-emr/77140?camid=4v1a](www.igi-global.com/chapter/effects-electronic-medical-record-emr/77140?camid=4v1a)