Chapter 62
A Viewpoint of Security for Digital Health Care in the United States:
What's There? What Works? What's Needed?

Steven A. Demurjian
University of Connecticut, USA

Solomon Berhe
University of Connecticut, USA

Alberto De la Rosa Algarín
University of Connecticut, USA

Thomas Agresta
University of Connecticut Health Center, USA

Jinbo Bi
University of Connecticut, USA

Xiaoyan Wang
University of Connecticut Health Center, USA

Michael Blechner
University of Connecticut Health Center, USA

ABSTRACT

In health care, patient information of interest to health providers, researchers, public health researchers, insurers, patients, etc., is stored in different locations via electronic media and/or hard-copy formats. All potential users need electronic access to health information technology systems such as: electronic health records, personal health records, patient portals, and ancillary systems such as imaging, laboratory, pharmacy, etc. Controlling access to information from multiple systems requires granularity levels of privileges ranging from one patient to a cohort to an entire population. In this paper, we present a viewpoint of the state of secure digital health care in the United States, focusing on the resources that need to be protected as dictated by legal entities and regulations, the available approaches in the present state-of-the art, and, the potential needs for the future of security for digital health care. By utilizing a real world scenario, the authors explore the limitations of health information exchange in the United States, and present one possible architecture for secure digital health care that builds on existing technology alternatives.

DOI: 10.4018/978-1-4666-8756-1.ch062

1. INTRODUCTION

Over twenty years ago, two articles related to health care security were published that were noteworthy for the time. In (Biskup, 1990), privacy and confidentiality in medical information systems was explored, advocating a role-based approach, and detailing the state-of-the-art in available systems. In (Ting, 1990), a case study of mental health delivery from information and semantic perspectives was presented, providing scenarios of usage of information by physicians, nurses, etc., and promoting a role-based approach as the most appropriate solution. What is surprising is what has stayed the same and what has changed over the last 20 plus years in the health care domain in terms of tracking patient care (via paper or electronic form) and facilitating secure information exchange as a patient transitions between care settings, more specifically in the United States. For instance, in 1990, would anyone have predicted the introduction of the Health Insurance Portability and Accountability Act[1] of 1996 (HIPAA) Privacy and Security Rules for protected health information? At the time, health care delivery was based more on paper than electronic health records (EHRs). How about the Genetic Information Non-discrimination Act (GINA)[2] of 2008? GINA aims to protect a patient's genetic information against discrimination in health insurance and employment. Or even the Ethical, Legal and Social Implications (ELSI) research program? ELSI was introduced to manage genomic data for personalized medicine. There have also been dramatic changes in patient care, including: EHRs in some medical doctor offices ("implementation rates reached 68% in family practices in 2011"[3] while "just 27% of physicians used EHRs with multi-functional capabilities"[4]); and, personal health records (PHRs) for patients to store their own health information (and download medications from a pharmacy, share data with providers, etc.). Evolving needs for health care delivery include a Patient Centered Medical Home[5] where one provider coordinates care for patients with chronic diseases; an accountable care organization (ACOs)[6] to coordinate providers regarding Medicare patients with chronic conditions; and the upcoming Meaningful Use Stage 2[7] capability for patients to be able to view, download, and transmit their records which will require the development of a standardized transmission of all types of medical information. These three and other evolving initiatives will require secure data collection from multiple health information technology (HIT) systems.

The harsh realities in health care and HIT adoption in the United States are: the limited capabilities of health information exchange (HIE) among all of these various data sources; the high number of providers that are predominately paper based with limited or no access to EHRs or other HIT systems; and, the fact that security is often an afterthought in this process, supported for individual systems for specific providers, but overlooked when one attempts to bring together patient data from multiple electronic sources. In patient centered medical homes, the effective care of a diabetes patient with high blood pressure may involve the family practitioner (who sees the patient regularly), an endocrinologist (if diabetes is complex in its manifestation), a cardiologist (diabetes patients often have heart disease), and a nutritionist (for managing diet or dealing with obesity). These four providers may have different EHRs (or none) and an inability to share data (patient history, lab test results, etc.) to facilitate the required care. The access needs to be integrated (electronic sources), secure (individual sources and across the integrated sources), and collaborative (individuals can view/update same patient record simultaneously). Our main objective in this paper is to enumerate prevalent issues for secure, integrated, and collaborative health care in the United States, requiring us to provide a roadmap for secure digital health care in the not so distant future. Our viewpoint is intended to answer questions such as: what patient information is available for each source, how can