Chapter 8
Privacy Considerations for Electronic Health Records

Mary Kuehler
University of Tulsa, USA

Nakeisha Schimke
University of Tulsa, USA

John Hale
University of Tulsa, USA

ABSTRACT

Electronic Health Record (EHR) systems are a powerful tool for healthcare providers and patients. Both groups benefit from unified, easily accessible record management; however, EHR systems also bring new threats to patient privacy. The reach of electronic patient data extends far beyond the healthcare realm. Patients are managing their own health records through personal health record (PHR) service providers, and businesses outside of the healthcare industry are finding themselves increasingly linked to medical data. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and other regulatory measures establish baseline standards for protecting patient privacy, but the inclusion of medical images in patient records presents unique challenges. Medical images often require specialized management tools, and some medical images may reveal a patient's identity or medical condition through re-linkage or inherent identifiability. After exploring EHR systems in-depth and reviewing health information policy, the chapter explores how privacy challenges associated with EHR systems and medical images can be mitigated through the combined efforts of technology, policy, and legislation designed to reduce the risk of re-identification.

DOI: 10.4018/978-1-61350-501-4.ch008

INTRODUCTION

Electronic Health Record (EHR) systems promise to reduce the cost of healthcare while improving patient care. Through the American Recovery and Reinvestment Act of 2009, the U.S. government allocated $19.2 billion to improve health information technology, primarily by encouraging widespread adoption of EHR systems (HITECH Answers, 2010). Eliminating administrative overhead and improving medical record workflow help reduce human error and improve the quality of service. Moreover, the transition to EHR systems offers great potential for collaboration and data sharing, enabling medical research and knowledge discovery on a global scale. This is especially true for efforts where large-scale collection is limited by cost and subject enrollment. For example, the Alzheimer's Disease Neuroimaging Initiative (ADNI), a multisite collaborative research effort, has collected images from over 40 sites and distributed data to more than 1,300 investigators to date (Kolata, 2010; Mueller, et al., 2005). The success of ADNI has led to the establishment of similar efforts for Parkinson's disease.

Along with the push for medical entities to utilize EHR systems comes a heightened threat to the privacy of patient medical data. In the U.S., regulation of patient privacy in EHR systems falls under the Health Insurance Portability and Accountability Act (HIPAA), which defines protected health information (PHI) and how it can be used. Improvements in technology have enabled EHR systems to incorporate medical images alongside data found in traditional paper charts. As the capabilities of capturing medical images progress, privacy measures and regulations regarding electronic medical data must also advance to encompass these images.

Discussions of patient privacy are often confined to the realm of healthcare and insurance providers, but the subtleties of the prevailing industry environment concerning medical data extend far beyond entities that are legally required to protect patient privacy. Businesses that are not subject to healthcare privacy laws also handle medical data, often unknowingly, when employees manage and disseminate health information using company resources. This may expose the company to potential liability. Beyond EHR systems, other sources may disclose PHI, such as Internet search terms or calendar appointments. These incidental exposures, along with the inherent privacy risks posed by certain classes of medical images, should be considered as much a threat to privacy as an EHR system data breach within the healthcare industry. It is essential that businesses and consumers be made aware of these issues.

This chapter gives an overview of EHR systems and explores health information privacy in the context of two emerging themes — the expanding reach of PHI, and the proliferation of medical images. Policy, technology and organizational solutions are considered to help enterprises within healthcare and beyond meet the challenges they present.

BACKGROUND

EHR Systems

EHR systems store a wide range of patient data and information types — patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports (HIMSS, 2010). The information in an EHR is stored as either structured or semi-structured data. Structured data refers to information in pre-determined data fields with a finite set of acceptable input. Semi-structured data allows for the input of free-text responses by the medical professional.

Fields with a predetermined list of acceptable input are advantageous within an EHR system because there is no ambiguity concerning the data collected. The pervasiveness of medical coding is a great example of how structured data is used