Chapter 72
Legal and Ethical Considerations in the Implementation of Electronic Health Records

Karen Ervin
Pennsylvania Hospital Librarian, USA

ABSTRACT

This chapter examines the literature of healthcare in the United States during the transitioning to electronic records. Key government legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), which were part of the American Recovery and Reinvestment Act (ARRA) and the Affordable Health Care Act, are reviewed. The review concentrates on patient privacy issues, how they have been addressed in these acts, and what recommendations for improvement have been found in the literature. A comparison of the adoption of electronic health records on a nationwide scale in three countries is included. England, Australia, and the United States are all embarking in and are at different stages of implementing nationwide electronic health database systems. The resources used in locating relevant literature were PubMed, Medline, Highwire Press, State Library of Pennsylvania, and Google Scholar databases.

ORGANIZATION BACKGROUND

Legal and ethical issues regarding patient confidentiality in the adoption of electronic health records in the United States are the focus of this paper. The Privacy Rule, which protects all "individually identifiable health information" held in any form, is one of the most central and well known parts of the HIPAA Act (U.S. DHHS, 1996, p.1). Also, important are both the Affordable Care Act and the HITECH Act that deal with Medicare and Medicaid expansion ("HITECH," 2009). Additionally, the first phase of the Obama Administration's HITECH Act, which provides financial incentives to health care organizations that adopt and use electronic health records by the end of 2012, was put into law, effective in February 2009. The goal of obtaining over 100,000

DOI: 10.4018/978-1-4666-8756-1.ch072

health care providers using electronic health records (EHRs) by the end of 2012 has already been exceeded (Centers, 2012). Consequently, many hospitals and medical practices across the nation are confronted with the proper handling of electronic records to ensure patient confidentiality even before the legal and ethical ramifications have been critically discussed.

SETTING THE STAGE

The literature that investigates the process of automating patient records and confidentiality, as defined in the HIPAA Act, must be explored in order to address questions of legal and ethical aspects involved. In order to address the confidentiality concerns one needs to understand the similarities and differences between electronic and paper records and to define exactly what is contained in each type. According to the Council on Ethical and Judicial Affairs (CEJA) of the American Medical Association (AMA), electronic medical records, also called electronic health records (and referred to as EHR hereafter), "are not merely digitized versions of paper records" (Sade, 2010, p. 40). Electronic records contain "large amounts of highly detailed clinical information," they are extremely compact, can be easily stored and rapidly transmitted between healthcare professionals and institutions (Sade, 2010, p. 40). Paper medical records do not present these characteristics; they are usually official forms and charts found in one central location, limited to each institution housing its own set of records for each individual served by the organization. Breaches of paper records usually do not occur outside of or beyond the individual organization. The potential for breaches of electronic records is much greater due to their inherent vulnerability. The characteristics which make them so attractive (ease of use, rapid transmission between providers, etc.) also make them potentially vulnerable. The USA Patriot Act of 2001 and the renewal of the law in 2006, made it legal for the FBI to search confidential medical records as part of counterterrorism efforts (Landa, 2006). The HIPAA Privacy Rule does not restrict disclosure of de-identified health information, which may be used by law enforcement officials, making it easier for these officials to have access to private health information, without the knowledge or consent of the patient. The AMA Council on Ethical and Judicial Affairs does not address this concern at all (Sade, 2010).

In order to fully appreciate what is considered protected health information, one must read the statement on confidentiality or at least the Summary of the HIPAA Privacy Rule (U.S. DHHS, 1996). Protected health information refers to the protection of all "individually identifiable health information" held or transmitted by a covered entity or its business associates. This includes all forms: paper, electronic, and oral.

Individually identifiable health information is information, including demographics, that relates to:

1. The individual's past, present or future physical or mental health or condition.
2. The provision of health care to the individual.
3. The past, present or future payment for the provision of health care to the individual (U.S. DHHS, 1996, p. 1).

This information either identifies the individual or can be used to identify them. It includes common identifiers such as name, address, date of birth, and social security number. Excluded from protection are employment records that a covered entity (employer, insurance company) maintains in its capacity as employer, and "certain other records…defined in the Family Educational Rights and Privacy Act" (U.S. DHHS, 1996, p. 1). There are no restrictions on the use or disclosure of de-identified health information. De-identified information refers to health information that has been de-identified either by a formal determination by a qualified statistician, or by the removal