Chapter 3
Hippocratic Database and Active Enforcement

Terry Dillard
Dillard Systems, LLC

ABSTRACT

There are an increasing number of laws and statutes being passed globally to protect the privacy of sensitive healthcare information. This complexity of legislation creates legal concerns for those stakeholders in the healthcare systems that collect and store this sensitive data. This chapter seeks to explore some technology based solutions for managing these complexities and that aim to mitigate some of the potential legal concerns associated with these activities.

INTRODUCTION

Governments across the globe are establishing data protection laws that constrain the disclosure and processing of personally identifiable information. These laws impose custodial and pecuniary burdens upon organizations that manage personal information, and may hinder the legitimate sharing and examination of information (Johnson & Grandison, 2007).

DOI: 10.4018/978-1-60960-174-4.ch003

Member states within the European Union are required under the Directive on Data Protection to establish laws that impose rigorous limitations upon the processing of personally identifiable information (European Union, 1995). The United States, Canada, Australia, and Japan also followed suit to protect the privacy and security of personal data. These laws play a major and defining role in the management, sharing, and analysis of electronic health records (Agrawal & Johnson, 2007).

As the number of organizations and governments collecting personal information continues to grow at an unprecedented rate, individuals are

ever more exposed to the unauthorized disclosure, misuse, or abuse of their personal information, which increases the risk of medical or financial identity theft, injury to their reputation, or loss of personal privacy. Failure to adequately protect information could lead to organizations exposing themselves to civil and governmental liabilities due to negligence. However, failure to protect personal information within electronic health records could also restrain researchers from having access to data, therefore diminishing the potential for innovation, efficiencies, and medical breakthroughs (Solove, 2004).

Despite the growing number of countries that have enacted data and privacy protection laws, security breaches resulting in data, privacy loss, and identity theft seems to be at an all time high. This is primarily due to ineffective enforcement or execution of data protection policies within organizations, may they be within government or the private sector. Also, due to differing constitutional standards and cultural attitudes on the need to protect privacy, disparities exists within legal protections between different countries, which poses obstacles to the free flow of information to researchers, as well as the global economy (Johnson & Grandison, 2007).

Technology-based privacy solutions can be employed to address many of these obstacles by restricting the access and exposure of sensitive personal information stored within information systems. Such privacy technologies must have the ability to accommodate or adapt the complexities of heterogeneous data protection laws, by discretely handling each information element. To be effective, solutions need to accomplish this task without egregiously constraining legitimate or bona fide disclosure of information. Effective solutions must also be cost-effective and computationally compatible with existing information systems infrastructure, which reduces the overall burden of solution implementation and execution (Grandison, Ganta, Braun, & Kaufman, 2007).

HIPPOCRATIC OATH, CONFIDENTIALITY AND BENEFICENCE

The Hippocratic oath is a solemn promise that was required of physicians entering the medical profession, which can be trailed back to the Greek physician and teacher, Hippocrates (403 B.C.). Within the oath, physicians were firmly admonished to maintain appropriate decorum and privacy in the execution of their calling as physicians by refraining from the practice of disseminating what they saw or heard regarding the treatment of patients. Maintaining the confidentiality of the physician-patient relationship was essential to the ethical exercise of the profession (Eliot, 1910).

Confidentiality is most conspicuous within medical ethics, and is inextricably linked to the four founding principles of the Hippocratic oath, which are: (1) autonomy, the principle that expresses that personal data must not be disseminated in an unauthorized fashion. Each individual has the sovereign right to determine who may receive, store, and transmit their personal information; (2) Self-determination, which is the ability to circumscribe or restrict access to one's personal data; (3) Informed consent is the courtesy that must be extended to individuals prior to distributing any medical data to others; and (4) Non-malfeasance, which is the principle of doing no harm. Disclosing private information about patients could violate individual rights, and could produce harmful consequences, such as family members, friends, health care organizations, insurance companies, employers, or researchers misusing data in such a way as to violate individual preferences (Beauchamp & Childress, 2001). Therefore, the Hippocratic oath seeks to uphold confidentiality through the overarching principle of beneficence, which encapsulates all four founding principles (Neitzke, 2007).