Chapter 9
Scrutinizing the Rule:
Privacy Realization in HIPAA

S. Al-Fedaghi
Kuwait University, Kuwait

ABSTRACT

Privacy policies, laws, and guidelines have been cultivated based on overly verbose specifications. This article claims that privacy regulations lend themselves to a firmer language based on a model of flow of personal identifiable information. The model specifies a limited number of situations and acts on personal identifiable information. As an application of the model, the model is applied to portions of the Privacy Rule of Health Insurance Portability and Accountability Act (HIPAA).

INTRODUCTION

The notion of privacy is becoming an important feature of modern society. In this context, deciding how to regulate the processing of personal identifiable information (PII) is a vital issue. Responding to the public's awareness of the importance of protecting privacy of personal identifiable information, guidelines have evolved and converged around a set of basic privacy principles (e.g., OECD, 1980). How successful are these privacy principles? According to the OECD (1980) report,

The choice of core principles and their appropriate level of detail presents difficulties… In particular, it is difficult to draw a clear dividing line between the level of basic principles or objectives and lower level "machinery" questions which should be left to domestic implementation. (I. GENERAL BACKGROUND, 19, e)

According to Bennett (2001), privacy principles enfold different interpretations,

There are disputes for example: about … the distinction between collection, use and disclosure of information, and whether indeed these distinctions make sense and should not be subsumed under the overarching concept of "processing" … How these and other statutory issues are dealt with will, of course, have profound implications for the implementation of privacy protection standards within any one jurisdiction.(p. 12)

Mechanisms to protect the privacy of personal identifiable information include legal measures, policies and privacy-enhancing technologies. Legislations such as the Health Insurance Portability and Accountability Act (HIPAA) and systems such as P3P are not sufficient to safeguard privacy because "they do not address how personal data is actually handled after it is collected" (He & Antón, 2003, p. 1). Also, according to Fischer-Hübner and Ott (1998, p. 1) "privacy cannot be efficiently implemented solely by legislative means. Data protection commissioners are therefore demanding that legal privacy requirements should be technically enforced and should be design criteria for information systems."

Among types of personal identifiable information, health information is ranked as being the most sensitive, at the same level as financial information (GPC Alberta, 2003). In the health information area, "Survey research found that the public … was deeply worried about how their personal medical information was being accessed and used in other sectors, for secondary purposes such as insurance, employment, licensing, research, law enforcement, public health, and media activities" (Westin & Gelder, 2005, p. 4).

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the most significant health care legislation in U.S. history. The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule (45 CFR Parts 160 and 164) to implement the requirement of HIPAA. According to U.S. Department of Health & Human Services (2003), "The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information" (HSS, 2003).

While privacy laws have an important role, other approaches are valuable. The "Privacy by Design" approach that incorporates the Fair Information Practices standards into information systems, tries to go beyond the HIPAA Privacy Rule (Westin & Gelder, 2005, p. 6). Nevertheless, it is also important to develop clearly defined privacy terms. Recent developments in the areas of privacy and information assurance have placed the elements of information privacy on firmer theoretical ground. This includes a model for personal information flow (Al-Fedaghi, 2006) that systematically categorizes subprocesses involved in personal information processing. This article illustrates a sample of the benefits of such an approach through inspecting portions of the Privacy Rule of HIPAA. Our purpose is not to take a position on any of the privacy principles or subprinciples, and neither is it to highlight conflicts and contradictions, but rather it is to provide precise specifications of privacy notions in order to apply them to different privacy standards, legislations, or codes of practice. Understanding the constitutive elements of privacy principles will help to determine any disparities and consistencies/inconsistencies when incorporating them in different laws and in their interaction with other requirements (e.g., enforcement mechanisms).

Personal Identifiable Information

This section focuses on personal identifiable information (PII) as our main object of study, and its flow model (Al-Fedaghi, 2005a, 2006). It is typically claimed that what makes the data "private" or "personal" is either specific legislation, for example, a company must not disclose information about their employees; or individual agreements, for example, a customer has agreed to an electronic retailer's privacy policy. However, this line of thought blurs the difference between personal identifiable information and other "private" or "personal" information. Personal identifiable information has an "objective" definition in the sense that it is independent of such authorities as legislation or agreement.