Abstract

Security Vulnerabilities and Conflicts of Interest in the Provider-Clearinghouse*-Payer Model

Andy Podgurski and Bret Kiraly
Electrical Engineering and Computer Science Department
&
Sharona Hoffman
School of Law
Case Western Reserve University
Olin Building
10900 Euclid Avenue
Cleveland, OH 44106
podgurski@case.edu, bdk6@case.edu, sxh@case.edu

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a national standard for electronic transfers of health data. It thereby fostered the development of new business relationships and more efficient modes of communication between health care providers, health plans (organizations such as insurance companies that pay for health care services), and health care clearinghouses (organizations providing value-added services). In addition, HIPAA seeks to ensure the confidentiality, integrity, and availability of health care information. In particular, the HIPAA Privacy Rule is a set of regulations intended to protect individuals' health information and to provide them with some control over its dissemination, and the HIPAA Security Rule specifies a series of administrative, technical, and physical security procedures for organizations to use to assure the confidentiality of electronic health information.

The HIPAA Electronic Transactions and Code Set Standards establish standard electronic formats for the exchange of health care information. The implementation of these standards brought a substantial degree of uniformity to electronic communications in the health care industry. In conjunction with the development of the Internet, the standards have given rise to an important new model for interaction between health care providers, payers (health plans), and clearinghouses, which is based upon a virtual intra-industry communication network connecting these entities. We call this the *Provider-Clearinghouse*-Payer* (*PC*P*) *model*. The PC*P model characterizes the information flows between providers, clearinghouses, and payers, the activities carried out by these organizations, and the personnel roles associated with these activities.

We present an analysis of threats to the confidentiality, integrity, and availability of electronic personal health information that are inherent in the PC*P model. We focus on threats involving the abuse of health information by providers, payers, clearinghouses, or their personnel rather than on generic computer security threats involving outsiders, which are dealt with extensively elsewhere. We give special attention to possible

conflicts of interest associated with the PC*P model and to the security threats they engender. We also examine the extent to which these threats may be magnified by conspiracy between organizations or individuals.

Having identified security threats inherent to the PC*P model, we examine the extent to which these threats are mitigated by application of the HIPAA Security Rule during design, implementation, and maintenance of a computer system conforming to the model. We show that a number of serious threats are *not* well mitigated by the Security Rule due to lack of technical specificity or completeness, which makes threat mitigation highly dependent on how an organization chooses to interpret the rule. We make a number of recommendations for improving the technical specificity of the Security Rule without unduly constraining implementers. In general, these recommendations focus on: (1) limiting the ability of employees of health care organizations to collect and disseminate electronic personal health information to unauthorized parties, (2) enhancing the ability of authorities to audit employee computer activities involving such information, and (3) preventing repudiation of improper activities. We argue that to provide reasonable assurance of privacy, it is necessary to impose significant restrictions on the means by which employees of health care organizations are permitted to access personal health information.

Although technical means can help to ensure that personal health information is not abused, they are not sufficient to prevent such abuse, especially if organizations or individuals are willing to violate privacy regulations, exploit perceived ambiguities in them, or traffic in health information that may have been obtained illegally. Therefore, we also present an analysis of the *legal* issues raised by limitations of the HIPAA Security Rule. Notably, we argue that civil money penalties for HIPAA violations should be adjusted based on the *size* of a violating organization, in order to create appropriate deterrence for both small and large violators. In addition, we argue that special provisions, which may be outside the scope of HIPAA, are needed to prevent the creation of a *market* for illegally obtained electronic health information, involving employers, insurers, and other third parties.