



Security & Privacy Implications

*Of the Health Insurance Portability and Accountability Act
of 1996*

Table of Contents

Overview	1
Security and Privacy Implications of HIPAA	1
Conclusion	2
How EDS Can Help	3

Overview

The patient, health plan member and consumer point of view that permeates the HIPAA regulatory environment will be one that says, "use my personal health information to treat my illness and pay my insurance claim, but I will not automatically agree to your use of my medical records in ways that do not directly benefit me."

EDS Security and Privacy Services helps healthcare institutions understand and comply with the challenges of implementing HIPAA.

Security and Privacy Implications of HIPAA

The protection of the confidentiality of personal medical records is being highlighted as one of the critical mandates of the U.S. government. As part of an effort to guard the privacy rights of individual citizens, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will hold any organization that maintains individually identifiable health information (HIPAA protected information) responsible for implementing effective security and privacy policies and standards within their respective organizations. Activities such as the *anonymous* aggregation of patient histories for the purpose of deriving accurate statistical probabilities of success of various treatments are not covered by HIPAA as long as the personally identifiable fields are cleansed.

The final HIPAA Privacy Regulations were issued in April 2001 with compliance by covered entities required by 2003. Although the HIPAA Security regulations are still in proposed form they complement the privacy regulations and are also expected to be final in 2001. The larger scope of HIPAA provisions regarding transmission standards and other key content tasks were approved by the Department of Health and Human Services in August 2000.

From the perspective of a casual observer, some of the likely requirements for covered entities are straightforward. For example, businesses will need to do the following regarding HIPAA protected health information:

- Ensure that handlers of sensitive patient data have a legitimate business reason to do so
- Log transactions involving this information so that activities can be

traced back to employees who created or access it

- Limit access to the data so that employees cannot use it for improper purposes like selling it to third parties
- Force strong encryption protection on transactions that travel over the Internet or other public networks.

While these basic requirements are easy to justify for compliance with the HIPAA regulations, the logistical headaches of implementing them require a lengthy window of time in which to plan, test, and execute these changes.

One common misconception regarding HIPAA compliance for the Security and Privacy requirements is that the anticipated solutions are primarily technology driven and are completely dependent upon improvements in existing medical industry applications using software, hardware and network. To the contrary, many of the provisions involve an organization's willingness to drive security and privacy issues through the employee ranks and provide specific education and training on these topics. Only part of the training will relate to the use of company-wide applications. Another component deals with the issues of privacy from the *individual's* point of view. This point of view that permeates the HIPAA regulatory environment will be one that says, "use my personal health information to treat my illness and pay my insurance claim, but I will not automatically agree to your use of my medical records in ways that do not directly benefit me."

Other organization, such as pharmaceutical companies, academic medical institutions and drug testing companies who maintain individually

identifiable health records of patients who have been prescribed a drug or participated in research projects or clinical trials are handling HIPAA protected information and must comply with the regulations. In some instances medical records are impossible to de-identify for instance, when a patient has a rare and/or infectious disease and must be easy to locate. In these instances special handling of this data becomes extremely important to the organization and the patient.

Companies are required by HIPAA to create and enforce internal administrative policies and procedures that foster compliance with the Security and Privacy regulations. Employees will need to follow a prescribed course of activities (and refrain from non-prescribed activities) in order to meet these high privacy standards. These employee activities will need to be carefully identified and scrutinized by senior management and implemented across all business units in a uniform manner that ensures that later audits by the government reveal a good faith compliance effort. Employees who do not comply with HIPAA regulations are personally subject to fines and prison terms without the protection of the traditional "corporate veil" that shields individual employees from responsibility for illegal activities in the course of their employment duties.

It should be noted that instances might exist in which HIPAA regulations may be superseded by individual state regulations that are more stringent than the federal standards. Companies will be responsible for determining whether state or federal laws are more applicable to their business

environment.

The first step that an organization should take in preparation for their HIPAA compliance effort is to appoint a high level Security and a Privacy Manager or combination thereof. These individuals should then work together to appoint a committee of business and IT managers throughout the organization who are likely to provide useful input or will take responsibility for implementation tasks. One of the first tasks to be carried out by this committee will be to conduct company-wide assessments of the state of security and privacy in order to evaluate the effectiveness of their current environment. Whether conducted internally or through the assistance of an outside consulting organization such as EDS, the key output of these assessments will be a formal gap analysis that points out the company's strengths and weaknesses measured to industry "best practices". With the final HIPAA regulations on Security and Privacy going into effect covered entities will have a well-defined standard against which to measure their internal efforts.

Conclusion

The effective implementation of security and privacy measures will serve to minimize the chance that confidential patient records will be revealed accidentally through lax procedures, exposed databases, and a lack of integrity of the records themselves.

Resting on a foundation of secure business and information handling practices, privacy management within an organization will focus on the appropriate uses of gathered health information. Activities that are related

to the direct delivery of health services or the payment of claims are readily acceptable. Third-party transactions including names, addresses, and/or specific medical conditions of patients are prohibited unless a prior arrangement has been made *with the patient or by defined exceptions in federal (or state) laws* to permit the transfer of information not intended to benefit the patient in a direct or indirect way.

Making sense of the HIPAA regulations can be a daunting task for the Security and Privacy manager. The final privacy regulations are over 1500 pages in length. A number of companies are seeking outside expertise in interpreting these regulations, and EDS stands ready to assist by providing the specialized knowledge and experience needed to give our clients the confidence that their organizations will be ready to be measured successfully against the HIPAA standards. Success in complying with HIPAA Security/Privacy regulations will give our clients a competitive edge in the health care industry by giving consumers the confidence of knowing that the most personal details of their medical history are protected from undesired disclosure in the open market.

How EDS Security and Privacy Services Can Help

EDS has recruited some of the privacy and security industry's most talented professionals. Unlike many Big 5 and niche security boutiques, EDS Security and Privacy Services "has done this before." Security and privacy is our core competency – not just an add-on. EDS Security and Privacy Services is among the very few who understand the important relation between security and privacy. The following are just a few of the security and privacy experts that are providing the intellectual capital for EDS Security and Privacy Services:

Al Decker - Before coming to EDS Security and Privacy Services, Al founded and was CEO for Fiderus Strategic Security and Privacy Services. He also had served as the Worldwide Director of IBM Security and Privacy Services within IBM Global Services. Previous to IBM, Mr. Decker was a partner and the national director of IT Security Services at Coopers & Lybrand LLP.

Rebecca Whitener – Prior to coming to EDS Security and Privacy Services, Rebecca was co-founder of Fiderus Strategic Security and Privacy Services. Prior to that, Ms. Whitener was the former head of IBM's global privacy division and served as an appointed member of the Federal Trade Commission Advisory Committee for Online Access and Security.

Gail Magnuson – Gail was the director of the Fiderus Privacy Practice before coming to EDS Security and Privacy Services as a subject matter

expert and privacy consultant. Ms. Magnuson was the former Chief Privacy Officer to Bank of America and the leading architect of a number of industry privacy alliances including the Online Privacy Alliance and the Better Business Bureau's on-line Seal of Approval.

Sharmie Atwood – Sharmie joined the EDS Global Security and Privacy Services team from Fiderus and brings over 20 years of telecommunications information security expertise, software engineering and privacy subject matter expertise to EDS. While at Fiderus, where she was co-developer of the national privacy practice and was a principal consultant for privacy and security engagements that included companies affected by global privacy law and regulation and within healthcare, financial and self-regulating industries.

Peter Reid – Peter joined the EDS Global Security and Privacy Services team from Fiderus, where he was a principal of the national privacy practice, responsible for the delivery of privacy services to customers. He brings to EDS more than 30 years of international and multi-functional experience in the information-technology field, having worked in the U.S., Canada and the U.K. Mr. Reid is a former vice president of NCR Corporation's Privacy Center and a recognized expert in information privacy, particularly in the areas of customer relationship management (CRM) and data warehousing.

Saul Schiffman – Saul joined the EDS Global Security and Privacy

Services team from Fiderus, where he provided security and privacy services in a wide range of industries. Mr. Schiffman is a leader in privacy standards and security, with more than 30 years of combined experience in security and privacy standards and practices, organizational management, and hands-on architecture and design of secure networks and software systems.

Ken Barney - Ken joined EDS Global Security and Privacy Services from Fiderus where he was the Chief Knowledge Officer. Previous to that he was at IBM Global Services as an executive consultant in the Security and Privacy consulting practice. Before that, he was Vice President of Technology Risk Management for First Union National Bank.

About EDS

As a leader in the global information technology services industry for more than 35 years, EDS helps businesses and governments discover solutions that can improve their performance. Our services include consulting, electronic business, business process management and information technology. We form strong partnerships with our clients to create end-to-end capabilities and scalable solutions: from strategic planning to final implementation. In the end, what clients gain from us are ideas that work. Said another way, we apply our knowledge to help them profit. We serve the world's leading companies and governments from more than 800 offices and service facilities in more than 45 countries. Addresses, phone numbers and fax numbers are listed on the EDS Web site: www.eds.com/contacts.

Corporate Headquarters

United States
5400 Legacy Drive
Plano, Texas 75024
1 972 604 6000
www.eds.com

Regional Headquarters

Asia Pacific
Hong Kong

Canada
Toronto, Ontario

Europe and Africa
Uxbridge, Middlesex, UK

Latin America
São Paulo, Brazil

