



WORLD

DATA PROTECTION REPORT

Monthly news and analysis of data protection & privacy issues from around the world

■ UNITED STATES

“HIPAA” Hiccups – Privacy Standards for U.S. Health Care Information Force Data Protection Enhancements

By Mark Starcher, President, Scanmark Limited, McLean VA.

In the not-too-distant future, access to health care information in the United States will begin to resemble airline passenger security procedures adopted in the post-September 11 world. The concepts of biometric authentication, access control lists and “secure” areas will no longer be confined to air travel. Individuals are likely to face similar scenarios when interacting with U.S. health care providers and their business partners.

These changes in information access are being mandated by the Health Information Portability and Accountability Act,¹ the controversial health care legislation, designed to standardise and secure the transmission of electronic health care related information. The privacy regulations are part of a multi-part plan to enhance security, standardise transactions and generally improve the efficiencies in health care data handling.

Privacy Regulations

Title II, Section 264 of HIPAA provides that the Secretary of Health and Human Services promulgate regulations specifying “standards with respect to the privacy of individually identifiable health information”. Final regulations for the privacy rules were issued on December 28, 2000 (45 CFR Parts 160 through 164). 45 CFR §164.534(a) provides that health care providers and health plans must implement privacy standards by April 14, 2003. 45 CFR §164.534(b)(2) excepts small health plans (generally less than \$5 million in activity) which have until April 14, 2004 to comply.

These privacy provisions are grounded in U.S. congressional concerns on the dissemination of medical information for marketing and other purposes. In that respect, the privacy regulations are intertwined with the security provisions of Section 262 of HIPAA. These regulations are intended to provide an individual with the ability to protect his or her patient health informa-

tion (“PHI”) and allow for informed consent when such information is shared with third parties.

Security Regulations

Section 262 of HIPAA amends title XI of the Social Security Act (42 U.S.C. 1301, *et seq.*) by adding Section 1173(d), which provides for security standards for electronic health information. Sections 1173(d)(2)(A) and (B) specify that the security safeguards will “ensure the integrity and confidentiality of the information”, and protect against “unauthorized uses or disclosures of the information”.

Proposed regulations were issued for the security regulations in August of 1998 (45 CFR Part 142, *et seq.*). These regulations have yet to be finalised. Nonetheless, the proposed security regulations are being addressed in conjunction with the privacy regulations since both are intended to protect patient health information (PHI). The privacy regulations focus primarily on allowing a patient to make informed judgements regarding the dissemination of PHI, while the proposed security regulations deal with the protection of the PHI within health care organisations and related entities.

One apparent difference between the privacy and security provisions of HIPAA deals with the scope of their application. The privacy regulations apply to any covered entity that handles medical information (regardless of format). Security provisions under the proposed regulations apply to all health care information *electronically maintained or used in an electronic transmission* (emphasis added). Hence, the security provisions do not appear to apply to paper – or film-based (fiche) medical records.

Although the privacy and security restrictions are conceptually sound, the “devil in the details” aspect of these regulations will result in operational hiccups and delays in accessing health care related information. For those seeking access to U.S. medical information, the privacy and security regulations may require a rethinking of access and security methods.

Overview

This article briefly touches on the implications of the privacy and security regulations for those persons that access PHI. Given the breadth of HIPAA's scope (its applicability to "business partners"²), new limitations on access to PHI will extend beyond the traditional health care industry. Banks, lawyers, insurance agents, pharmacists, eye-care professionals, cellular telephone companies, Internet Service Providers (ISPs), transportation services (taxis, ambulance services) and others may all be effected by these regulations because of their business relationships with health care or health insurance providers (the so-called "covered entities").

Business Processes and Due Diligence

The complexity of the health care industry leaves both privacy and security policies very ill-defined in terms of specific guidance. In the absence of more specific guidance, these regulations do make clear that a standard of care ("due diligence") will be imposed on health care (and related) entities in formulating privacy and security issues. Hence, the specific privacy and security procedures decided upon by an institution may not be as important as the business process used to arrive at these procedures. The management and business processes for a covered entity thus are a focal point for these regulations.

We can view the HIPAA privacy and security standards as analogous to traditional information system security plans, which are discussed briefly below. In many instances, these policies are in place but may simply need to be updated or refreshed to take into account recent technology (e.g., wireless networks) that permit more widespread access to protected health information.

Quantifying the Value of Information Assets

The formulation of the security/privacy standard business processes are analogous to the formalisation of privacy/security plans. Information security formulation is a business process where potential weaknesses within an organisation are identified. The security process is designed to preserve the business value of information by providing for:

- confidentiality;
- accuracy; and
- availability.

Information *confidentiality* is defined as providing a system allowing information to be shared amongst those that need access. The value of confidential information can be determined based on the financial impact to the entity of public release of that information.

Information *accuracy* consists of assuring that an information source is valid and assuring ongoing data integrity, *i.e.*, that the valid information source will not be corrupted or subject to unwarranted modifications.

Information *availability* assures ongoing access for users to appropriate information, *i.e.*, preventing so called denial of service to those who require access.³ Availability also covers the disaster recovery issues and associated planning.

Privacy/Security Policies and Procedures

Beyond these basic information security tenets, a plan must also address the business process of formulating and modifying security and privacy policies. This process can be broken down into five-steps:

- inspection;
- protection;
- detection;
- reaction; and
- reflection/feedback.

Inspection is the business process of identifying information assets, the capabilities of these information systems, and the interaction and value of those systems. In this phase, the organisation must do a system and data audit to identify all information sources (in any medium), their value to the organisation, current levels of protection, and future capabilities.

Protection involves the minimisation of risk through protection of selected assets, the provision for redundant systems, and other actions designed to provide cost effective security for information assets. The use of a cost/benefit analysis ties the level of security to the perceived value of the information assets.

Detection involves processes designed to identify, intercept and minimise any potential security breaches. This involves use of accepted security policies, virus and intrusion detection software, physical security devices (biometrics, secure access, ID cards, *etc.*) that may pinpoint potential security intrusions.

Reaction is the business process that comes in the aftermath of a security/privacy incident. This process includes procedures used to preserve evidence (computer forensics, physical evidence), and business continuity plans and must take into account all anticipated eventualities.

Reflection/feedback is the final phase of the security process and provides a "lessons learned" loop that allows the organisation to review and learn from previous security incidents and react and modify the ongoing security process. This step recognises the dynamic nature of this process.

Today's Business Environment

The processes outlined above are management tools designed to provide effective identification and quantification of potential risks and a process that will allow health care organisations to react to potential security risks.

These standards, however, need to be translated to everyday business interactions in order to access the impact of these new HIPAA privacy restrictions. Outlined below are samples of real world events that will likely

require modification to allow health care providers, insurers, and business partners to meet the guidelines of the HIPAA privacy and security mandates requirements. These are merely representative of the items that will come to light in a well-managed security and information asset audit. These actions are grouped by function:

External Communication

The privacy restrictions will generally apply to *all* external communications, *i.e.*, communicated in any medium, which retains or uses the protected health information.

E-mail

A simple example of the breadth of HIPAA involves the use of e-mail to correspond with third parties including patients, insurers, attorneys, government regulators and others. Any protected information captured in an e-mail and forwarded in an unencrypted format to an outside entity results in a privacy violation under HIPAA. This same argument also applies to the use of any instant message (IM) services.

Instant Messaging

Ironically, simply emailing or “IM-ing” a person with no identifiable health information could also be interpreted as providing protected information (the person’s e-mail address and IP address would appear to be protected under the privacy regulations). §164.504 defines individually identifiable health information expansively to include information that could be used directly or *indirectly* to identify an individual (emphasis added). §164.506(d)(2) of the Privacy Regulations provides a list of data elements that, if excluded from data sets, presume that the information has been “de-identified”, *i.e.*, capable of being used by third parties. Interestingly, one of these elements is *the email address and IP address of a recipient*. (emphasis added).

Hence, any interaction with a third party who coincidentally happens to retain protected information at the covered entity could violate the privacy rules.

This certainly speaks to a cogent e-mail retention policy and security policies that mandate encryption and/or deletion of e-mail and mail server logs. Even if encrypted, the e-mail address and IP address of the recipient would most likely be available, unless some sort of re-direct e-mail service was used to hide the source of the communication. This result stretches the limits of common sense.

Digital/Cellular Telephones

The use of third-party wireless devices (*i.e.*, those outside the control of the covered entity) could also violate privacy regulations.⁴ If, for example, a health professional used his or her cellular telephone to contact a patient, this communication could be viewed as subjecting the patient’s identity to risk. Although voice-to-voice communications are not viewed as protected health care information, cellular systems do capture telephone numbers and other call details for billing and

other purposes that, if obtained, could identify indirectly a protected person. This could lead to the unexpected result that third-party cellular telephone billing records companies become, in effect, protected health information.

Automated Appointment Services

In a related area, the use of automated appointment reminder services could also run afoul of the privacy restrictions in that these systems cannot guarantee the identity of the end user. For example, a voice mail left on an answering machine indicating that patient A has an appointment with cardiologist Dr. B, would violate privacy standards. Anyone with access to that answering machine could obtain this information.

The preamble to the privacy regulations indicated that protected health information does not include voice-to-voice or paper fax to paper fax transmissions, basing this conclusion on the fact that neither of these communications is stored on an electronic computing device. Information on these communications (*i.e.*, metadata or data describing these communications) is stored electronically and would appear to be subject to the privacy regulations.

Internet Service Providers

Similarly, use of an Internet Service Provider by a covered entity would result in a scenario where information that could be used to identify a third party (in this case the internet address of the user). This would further expand the scope of business partners to include the covered entity’s ISP. This is particularly true in a scenario where the ISP assumes responsibility beyond conduit services (*i.e.*, providing web hosting services, web design or other consulting services).

Fax Machines

This same argument could be used to include paper-to-paper fax machines in that the machine does capture information on call details. Fax-back systems, *i.e.*, fax communication between an end-user and a computer, are specifically included under systems covered by the definition of protected health information.

Again, the content of the voice or fax communication is irrelevant in this case. The simple act of placing a telephone call (or sending a fax) to a person with patient information at the covered entity could result in a privacy breach. Again, a common sense rule would limit the scope of HIPAA to exclude such a situation.

Personal Digital Assistants (PDAs)

On a related note, the use of Personal Digital Assistants (PDAs) in the health care business environment will likely be subject to significant limitations, including the implementation of network access controls and, when communicating through wireless connections, use of adequate encryption safeguards.⁵

Internal Access to Electronic PHI

Generally, communications within a covered entity will not require the use of encryption. The focal point for internal communications are the procedures used to authenticate and proscribe access to health-related information. Here, again, we look to well-formed IT security guidelines as the benchmark for in internal communication – the ability to limit access to information and the ability to authenticate the end user who happens to be accessing covered information.⁶

Use of standard IT security policies and methods are essential to compliance with HIPAA. In a risk assessment review of internal access and authentication, health care providers and related entities will need to consider, among others:

- passwords and password management;⁷
- the use of single sign-on applications;⁸
- the ability for applications to support automatic log-off commands;⁹ and
- restrictions on the use of access terminals in public areas.¹⁰

Both the privacy and security regulations also emphasise the need for documented disaster recovery plans to both minimise potential threats to PHI from natural disasters and also to allow patients the ability to access their PHI under most scenarios.

Physical Access Controls

Because the privacy regulations apply to PHI in any form, including oral, written and electronic records, significant physical security measures are essential to limit access to physical PHI records. For example: access controls including biometric and keypad activated electronic locks on file rooms, limited access fax areas, and access control lists for file folders are but several of many physical control items that must be considered.

Conclusion – Business Processes and Common Sense Should Control

The scope of these regulations appears daunting to most. The tenor of these rules, however, allow that those entities that follow structured business processes for identifying and dealing with privacy and security issues should be viewed as complying with the spirit of the law. In that context, the negligence standard of “business due diligence” would seem to apply. Common sense

should apply to reasonably limit the applicability of these rules.

1 Health Care Information Portability and Accountability Act (hereinafter “HIPAA”), P.L. 104–191, 104th Cong. (Aug. 21, 1996).

This article does not address the extensive transaction set and electronic interchange requirements set forth in 42 U.S.C. §1320d–2, as added by Title II, Section 262 of HIPAA.

2 As stated in the preamble to 45 CFR §164, et seq.:

The rules would create a sphere of privacy protection that includes covered entities who engage in treatment or payment, and the business partners they hire to assist them. While written consent for these activities would not be required, new restrictions on both internal uses and external disclosures would be put in place to protect the information.

See 45 CFR §164.506(e) for uses of private information by “business partners”.

3 For a more detailed overview of these concepts, see Pipkin, Donald L., *Information Security*, Hewlett-Packard Professional Books, Prentice Hall, Upper Saddle River, NJ, 2000, at pp. 13–18.

4 One would presume that use of an internal private telephone system (PBX) through a wired or wireless handset, would be defined as an internal communication that would be exempted from the privacy restrictions. The logs for these telephone calls, however, would be subject to privacy constraints and hence, would need to be secured.

5 The standard encryption algorithm used to secure wireless transmissions over the most widely used wireless network (the so-called “802.11b” wireless networking standard) has been broken. See ‘Off-the-shelf hack breaks wireless encryption’, CNN.com/Sci-Tech, August 11, 2001 www.cnn.com/2001/TECH/ptech/08/10/wireless.hack/ visited August 2, 2002. Hence, covered entities could require the use of secure encryption methods when communicating externally or internally through a wireless access point. Again, the standard here is one of due diligence. If an entity uses the standard encryption algorithm packaged in most wireless products, knowing that this encryption method has been compromised, could jeopardise any due diligence defence on the part of the PHI provider.

6 Examples of well-formed, customisable security policies can be found at the SANS Institute, an organisation that provides information and services relating to technology security: www.sans.org/newlook/resources/policies/policies.htm#template.

7 General guidelines for password security include passwords of no less than eight characters, including at least one numeric and one control [e.g., !@#%*&] character. These passwords should be changed every 90 days (or more frequently if possible). Audits should be regularly performed on password using password cracker software to weed out weak or patterned passwords.

8 Single sign on applications are software products that permit access to many different systems based on a single password or authentication event. Use of these applications will come under scrutiny as a result of the security provisions of HIPAA.

9 Automatic log-off refers to the ability of an application to close itself without human intervention based on a pre-defined “time-out” period. In the context of HIPAA, the time-out period will likely be tied to the location of the machine, i.e., machines located in public access areas will require shorter time-outs than those in restricted areas.

10 The placement of terminals in publicly accessible areas is questionable in light of HIPAA privacy standards.