
HIPAA Security Provisions:

Is Your Network Ready for a Physical?

- page 2** Introduction
- page 2** Initial Evaluation: Who, What and Why of HIPAA
- page 5** Vital Signs: Security Requirements Under the HIPAA Statute, Privacy Rule and Security Rule
- page 8** Doctor's Orders: Deadlines, Penalties and Sanction for Noncompliance
- page 8** Keeping PHI and Systems Healthy: A Prescription for HIPAA Compliance
- page 12** Conclusion: Maintaining Network Health Through Independent Change Auditing

Introduction

Most people know the formula for good physical health: eat right, exercise regularly and undergo an annual checkup. Fewer people, however, realize that federal law requires many businesses to follow procedures for good network “health,” especially when it comes to protecting personal medical information. Because a new set of security-focused regulations under the federal law known as the Health Insurance Portability and Accountability Act (HIPAA) becomes effective in April of 2005, many companies need to review the health of their systems that create, receive, transmit or maintain health information.

Is your company subject to HIPAA? If so, is it prepared to meet the requirements of the Security Rule? Like past (and possibly future) HIPAA regulations, April 2005 is the next compliance deadline for most entities covered by HIPAA, followed an April 2006 deadline for certain smaller entities. Because HIPAA and its rules can be amended, reinterpreted and supplemented, future deadlines may also arise. Read on to see whether your company’s systems are healthy enough to pass an internal security checkup, or are running the risk of a much more invasive examination by federal regulators and plaintiff’s lawyers.

Initial Evaluation: Who, What and Why of HIPAA

Just like a good physical examination begins with an initial evaluation of the patient’s appearance, height, weight and similar features, the establishment of baseline information like blood pressure and temperature, a good HIPAA compliance examination starts with an initial evaluation. Knowing who the law covers, what the law is and why it exists are good first steps toward compliance.

To summarize, HIPAA is a federal law that requires companies to adopt administrative, physical and technical measures to protect the confidentiality, integrity and availability of certain health information. The security section of HIPAA and a set of HIPAA regulations known as the Privacy Rule have, for some time, required companies to implement general security measures to protect health information. A new set of HIPAA regulations (known as the Security Rule) will become effective in April 2005. The Security Rule requires companies that create, receive, transmit or maintain health information in an electronic format to meet a much more detailed set of security standards than the HIPAA Privacy Rule. More details about the *who*, *what* and *why* of HIPAA are set forth below.

Who

HIPAA applies to entities that are defined in the law as “Covered Entities.” This term is defined in HIPAA to include:

- (1) Health Plans—plans that provide or pay for the cost of healthcare;
- (2) Health Care Clearinghouses—entities that process/facilitate information relating to an individual’s health, health care or health care payment; and
- (3) Health Care Providers—doctors, dentists, hospitals, clinics, medical groups or other providers of medical services that maintain or transmit health information in an electronic form.

¹ Daniel J. Langin is the principal of Daniel J. Langin, Attorney at Law, LLC. He has over 16 years of experience in private and corporate practice, including ten years of experience in technology, insurance coverage and intellectual property litigation and counseling. For more information, see www.langinlaw.com or contact Daniel at (913) 661-2430 or dlangin@langinlaw.com. This article is provided for general educational and informational purposes. It is not intended to provide legal advice.

At first blush, the term “Covered Entities” might seem to limit HIPAA to companies in the health care field. However, this definition creates one of the hidden compliance risks of HIPAA because the term “Health Plans” includes *nearly* all employer-sponsored group health plans. In fact, the Security Rule includes a separate section dedicated specifically to group health plans.²

Few employers, however, may be aware of their plan’s responsibilities under HIPAA, including the approaching compliance deadline for the Security Rule. A survey from April 2003 (the compliance deadline for the Privacy Rule) indicated that only 68% of Health Plans were HIPAA-compliant.³ Employers ultimately have de facto responsibility for HIPAA compliance because they sponsor and administer their Health Plans. From a practical perspective, this means that the definition of Health Plan expands the scope of HIPAA beyond health care companies to virtually any employer that sponsors a Health Plan for its employees.

What

Once a company determines whether or not it is subject to HIPAA, it needs to know what information the law covers. HIPAA applies to “Protected Health Information” (PHI), which is information that:

- (1) relates to the provision or payment of health care for an individual;
- (2) contains details that can be used to identify the individual (name, address, SSN, etc.), and;
- (3) is either created or received by a Covered Entity.

PHI can be created or received in a number of ways. These include not only obvious examples such as medical records or medical bills, but also employee health plan enrollment forms and claim payment or health savings plan information submitted to employee group health plans.

As noted below, the security provisions of the HIPAA statute and the Privacy Rule’s “mini-security rule” apply to PHI in paper, electronic or any other format. The Security Rule applies solely to PHI in an electronic format, whether in transit, residing on a network or stored in portable media.

Why

The “who” and the “what” of HIPAA give some clues about the “why.” HIPAA, the Privacy Rule and the Security Rule grew out of concerns that the computerization of medical information was subjecting it to a greater risk of unauthorized disclosure due to errors, misfeasance or computer exploits. HIPAA and its regulations were created to stop the negligent, intentional and sometimes careless manner in which private health information was being handled.

Between the April 14, 2003⁴ compliance deadline for the Privacy Rule and July 31, 2004, the government entity charged with enforcing the HIPAA Privacy Rule (the Office of Civil Rights, or OCR⁵) has received and initiated review of 7,577 HIPAA complaints. It has closed only 57% of those cases, most of them quietly (until recently—see the discussion of the Gibson case, below). One commentator suggested that HHS started slowly with HIPAA enforcement procedures to give Covered Entities more time to comply, provided that they had shown reasonable efforts to reach the deadline and were working with “all deliberate speed” towards achieving compliance.⁶

² 45 CFR 164.314.(b)(1)-(2).

³ HIMSS/Phoenix Health Systems Survey 2003 (available at www.hipaadvisory.com/action/surveynew/Spring2003.htm)

⁴ The compliance deadline for Small Health Plans (those that pay under \$5 million annually for health care) under the Privacy Rule was one year later, on April 14, 2004.

⁵ CMS is responsible for enforcement of the Security Rule.

⁶ Icenogle, “HIPAA Liability: Beware the Secondary Enforcers,” 103 *Wisconsin Medical Journal* No.1 (2004).

That “slow start” appears to have ended late in 2004 with the criminal conviction of a health care employee for violating HIPAA. The employee, Richard Gibson, apparently accessed records that enabled him to steal the identity of a patient and charge over \$9000 on four phony credit cards in the patient’s name.⁷ Although the prosecutor in the case recommended a moderate sentence of 12 months in prison, the judge gave Gibson 16 months and took the unusual step of ordering him to be immediately sent to prison.

The Gibson incident may indicate that the slow start for enforcement is over, and that HIPAA violations (including several thousand currently unresolved complaints) will be taken very seriously by the federal justice system. As one medical privacy publication noted, it takes time for enforcement efforts to bear fruit with HHS (just like any other bureaucracy), but it has won budgetary increases, hired new staff and appears to be prepared to ramp up enforcement efforts.⁸ Also, complaints sometimes take years to investigate and make their way through the regulatory process, so violations that occurred at the advent of HIPAA may just now be coming to light.⁹

The Gibson case also indicates—much to the surprise of some legal commentators—that individual employees of Covered Entities may be subject to criminal prosecution under HIPAA.¹⁰ Covered Entities face liability for the criminal acts of their employees, especially if they failed to develop adequate privacy protections over PHI.¹¹ At a minimum, a HIPAA violation by an employee of a Covered Entity is very likely to trigger an investigation of the Covered Entity’s HIPAA compliance by HHS. Even though that employee might be one bad apple in an otherwise innocent organization, HHS may find HIPAA violations by the Covered Entity if its lack of security enabled the employee to misuse PHI.

In addition to fines, penalties and prosecution, Covered Entities also need to be aware that plaintiff’s lawyers may act as “secondary enforcers” of HIPAA under civil law. Although HIPAA does not create a private right of action (i.e., a right for wronged persons to file civil suits under HIPAA), plaintiffs’ attorneys are likely to use HIPAA standards as the basis to establish negligence in civil cases involving medical information.¹²

A good example of a civil suit arising from wrongful access to health information is *Doe v. Medlantic Healthcare Group, Inc.*¹³ In the Doe case, a DC-area hospital was forced to pay a patient \$250,000 because the hospital’s poor computer security permitted an employee, who was not authorized to access medical records, to discover medical records showing that the patient was HIV positive. The employee told fellow employees about the patient’s HIV status, and the patient sued the hospital for invasion of privacy.

Similar medical privacy incidents have also yielded significant verdicts. For example, in February of 2003, a jury in West Virginia awarded a \$2.3 million judgment against an outpatient clinic of the University of West Virginia Medical Center because an employee of the clinic had accessed the medical records of three female

⁷ Tomlinson, “First HIPAA Conviction More Severe Than Expected,” November 5, 2004 (available at www.wrlaw.com/news_information/0/865/).

⁸ “OCR Viewed by Many as ‘Toothless’; How Aggressively Will It Enforce HIPAA?,” *Report on Patient Privacy*, June 2004 (Atlantic Information Services, Inc.) (quoting lawyer Mark Barnes) (available at <http://www.aishealth.com/Compliance/Hipaa/RPPOCRToothlessHowAggressive.html>).

⁹ See *Id.*

¹⁰ Hartsfield, “A HIPAA Wake-Up Call” (August 24, 2004) (available at www.hklaw.com/publications/newsletters).

¹¹ *Id.*

¹² Icenogle, “HIPAA Liability: Beware the Secondary Enforcers,” 103 *Wisconsin Medical Journal* No.1 (2004).

¹³ No. 97-CA3889 (D.C. Super. Ct. November 30, 1999).

patients and then discussed their medical information with third parties.¹⁴ In a simple “slip of the tongue” case, a fire department in Wisconsin was subjected to a \$33,000 verdict because one of its EMTs told a patient’s coworkers that the fire department had responded to a call concerning an apparent drug overdose by the patient.¹⁵ Although these incidents did not involve any breach of information security, these incidents could just as easily have involved access to electronic records and e-mail. Whether the data is accessed and revealed electronically or in physical form these cases demonstrate the potential size of medical privacy verdicts.

Vital Signs: Security Requirements Under the HIPAA Statute, Privacy Rule and Security Rule

The next step in any physical, after initially evaluating the patient, is reviewing vital signs such as temperature or blood pressure and comparing them to standards for such signs (normal temperature and blood pressure, for example). These vital signs reveal details that may not be apparent from an initial evaluation. In a similar fashion, the next step in a HIPAA compliance checkup is reviewing the “vital sign” standards for HIPAA compliance as established in the details of the HIPAA security provisions.

Just as certain vital signs (such as heart rate) may demand more attention than other vital signs, so it is with HIPAA compliance. In essence, HIPAA contains three separate but related security provisions. The HIPAA statute contains a general requirement for reasonable security, the Privacy Rule contains a “mini-security rule” that applies to both paper and electronic PHI, and the Security Rule contains the most detailed security provisions, which relate to PHI in electronic format. Of these three sets of regulations, the Security Rule demands the most immediate and detailed attention from an information security perspective.

The relevant security language of the HIPAA statute exists in section 1320d-2(d)(2). This section requires each Covered Entity to maintain reasonable and appropriate administrative, technical, and physical safeguards for three purposes:

- (1) to ensure integrity and confidentiality of PHI;
- (2) to protect against any reasonably anticipated threats or hazards to the security, integrity, or unauthorized uses or disclosures of PHI, and;
- (3) to ensure compliance by officers and employees of the Covered Entity with HIPAA.

These provisions have been effective longer than either the Security Rule or the Privacy Rule. Although they lack detail, in appropriate circumstances these could be used as a “catchall” provision to encompass security measures not named in either the Security Rule or the Privacy Rule, but which were otherwise “reasonable and appropriate” for the integrity, confidentiality or security of PHI.

The HIPAA Privacy Rule contains a provision known as the “mini-security rule.”¹⁶ This section requires Covered Entities to:

- (1) adopt appropriate administrative, technical, and physical safeguards to protect privacy of PHI; and
- (2) safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the Privacy Rule.

¹⁴ *K.C., et al. v. West Virginia Medical Corp., d/b/a University Health Associates*, Civil Action No. 99-C-509 (Circuit Court of Monongalia County, W.V. February 5, 2003).

¹⁵ *Pachowitz v. LeDoux*, 666 N.W.2d 88, 265 Wis. 2d. 631 (Ct. App. 2003).

¹⁶ 45 CFR 164.530(c)(1).

Like the security language of the HIPAA statute, this language is broad in scope but short on detail.

This raises an interesting question concerning the overlap of the security provisions of HIPAA: If a Covered Entity transmits or maintains PHI in *both* paper and electronic format, is it subject to the security provisions of the HIPAA statute and the Privacy Rule, or the provisions of the Security Rule, or all three? According to the preamble to the Privacy Rule, Covered Entities that transmit or maintain PHI in electronic form are subject to *all three* sets of provisions, with the caveat that the Security Rule only applies to electronic PHI. Because most Covered Entities maintain PHI in both paper and electronic formats, this essentially means that most Covered Entities are subject to all three sets of security provisions.

The most detailed of the three HIPAA security provisions is the Security Rule. It requires Covered Entities that transmit or maintain PHI in an electronic format to ensure the confidentiality, integrity and availability of PHI that the entity creates, receives, maintains or transmits in an electronic format. Much more detailed than the other HIPAA security provisions, it contains numerous standards and implementation specifications.

Like other recent security laws such as the Gramm-Leach-Bliley Act, the HIPAA security rule is divided into three categories of requirements, namely, administrative, technical and physical. The Security Rule is also divided into two types of implementation specifications: Those that are “addressable” (i.e., must be reviewed and considered for implementation, and reasons documented if not implemented) or “required” (i.e., *must* be implemented).

A sampling of the specifications reveals their complexity. The administrative requirements include the following steps:

- (1) Adoption of a security management process supported by policies and procedures to prevent, detect, contain and correct security violations, and which include:
 - a. Risk analysis: accurate and thorough assessment of risks and vulnerabilities to PHI;
 - b. Risk management: implementation of security measures sufficient to reduce these risks and vulnerabilities;
 - c. Information systems activity review: regular review of audit logs, reports, incident tracking, etc. The Security Rule also incorporates a mandatory reporting requirement for all “security incidents,” which the law defines to include both attempts and successful exploits;
 - d. Information access management: Policies and procedures to ensure that access to PHI is consistent with the restrictions of the Privacy Rule (making sure only authorized users access PHI, documenting such access, isolating clearinghouse functions from other functions of the Covered Entity, etc.);
 - e. Security incident response procedures, including mitigation and documentation of security incidents; and
 - f. A contingency plan (including a data backup plan), procedures to restore lost data, and an emergency mode operation plan that enables use of existing PHI while operating in emergency mode.

The physical requirements are similarly complex. In general, the Security Rule requires Covered Entities to adopt measures necessary to prevent physical access to electronic PHI wherever it may be located. Governing physical access to electronic information, however, necessarily involves the use of information technology and security measures such as proximity cards and the like. The implementation specifications include adoption of device and media controls that address accountability (i.e., recording movements of hardware and electronic media that contain or transmit/receive PHI) and data backup and storage (creation of a retrievable, exact copy of PHI).

Last, the Security Rule contains technical requirements. A sampling of these requirements includes the following:

- (1) Access controls: utilizing technologies that limit access to PHI to only those persons having access rights, including access procedures to obtain electronic PHI in an emergency;
- (2) Audit controls: utilizing hardware, software and procedures that record and examine activity in systems that contain or use electronic PHI; and
- (3) Integrity: utilizing procedures and mechanisms to detect and protect electronic PHI from alteration or destruction.

The key to understanding and implementing the Security Rule's numerous provisions lies in breaking the rule down into its three major implementation categories (administrative, physical and technical), all while understanding that the rule covers much more than security. The rule's provisions—whether administrative, physical or technical—all point to a comprehensive standard for protecting not only confidentiality, but also integrity and availability of electronic PHI. Protecting the security of PHI is a very good step towards compliance, but if systems and processes do not exist to ensure that the PHI is accurately maintained (integrity) and available upon demand, and to audit and track the status of electronic PHI, then compliance efforts will fall short.

A specific case that illustrates the value of auditing and tracking took place in 2002. A nurse who worked for Kaiser Permanente accessed Kaiser's records to check her adult daughter's medical billings (the daughter was insured by Kaiser) to discover whether her daughter was pregnant.¹⁷ The daughter discovered the mother's actions after her brother, who had been tipped off by the mother, asked his sister about her pregnancy. The daughter sued both Kaiser and her mother. Kaiser reached an amicable settlement of the case in arbitration, in part because it was able to track the extent of the mother's unauthorized access to her daughter's records from audit trails and to demonstrate that it was a limited occurrence by one bad actor (the mother). Stronger security procedures might have enabled Kaiser to avoid liability altogether, but at least the auditing and tracking systems enabled Kaiser to limit the loss to what Kaiser characterized as "minimal damage."¹⁸

In addition to the administrative, physical and technical requirements of the Security Rule, two other relevant provisions are worth mentioning. First, the organizational requirements of the Security Rule state that Covered entities must, by contract, require their "Business Associates" (i.e., contractors who handle electronic PHI) to implement the same kinds of administrative, physical and technical safeguards as the Covered Entity and report any security incidents to the Covered Entity. These Business Associates must extend the same requirements to their own subcontractors. Second, the documentation provisions of the Security Rule require Covered Entities to document all policies, procedures, actions, activities or assessments mandated by the Security Rule for a period of 6 years. Documentation may be in electronic form.

¹⁷ "Audit Trails Back Up HIPAA 'Minimum Necessary' Rule," (August 11, 2004) (available at www.aishealth.com/compliance/Hipaa/RMCAuditTrail.html)

¹⁸ Id.

The Doctor's Orders: Deadlines, Penalties and Sanctions for Noncompliance

No physical is complete unless the examining doctor tells the patient to drop a few bad habits and pick up some healthy ones. These discussions typically end when the doctor advised the patient of the consequences of failing to protect his or her health.

Just like physical health, inattention to network infrastructure health also has consequences. The penalties for noncompliance with HIPAA range up to 10 years in prison and \$250,000 for the most serious, intentional violations of HIPAA. As noted above in the discussion of the "why" behind HIPAA, secondary enforcement in the form of civil suits for violation of medical privacy could easily result in six- and seven-figure judgments.

The current and most pressing deadline for compliance is the first deadline for the Security Rule, which is April 20, 2005. A future deadline of April 20, 2006 exists for Small Health Plans. The deadlines for compliance with the security provisions of the HIPAA statute and the Privacy Rule have long since passed. Because HIPAA and its rules can be amended, reinterpreted and supplemented, future deadlines may also arise.

Although some argue that HIPAA compliance is not a priority because the government does not hold regular HIPAA examinations of Covered Entities, a much more likely scenario is that an employee or patient will blow the whistle on a non-compliant entity. This likelihood exists because the Privacy Rule requires Covered Entities to provide each patient (or in the case of employee group health plans, each employee) with a privacy notice that contains the contact information needed to file a HIPAA complaint with HHS. It only takes one disgruntled employee or unhappy patient to initiate a HIPAA investigation.¹⁹

Keeping PHI and Systems Healthy: A Prescription for HIPAA Compliance

In this age of daily drug breakthroughs, few patients leave a checkup without one or more prescriptions in hand. Whether the diagnosis is social anxiety, hair loss or brittle yellow toenails, doctors can usually provide their patients with a potential treatment and course of action to stay healthy.

Similarly, no discussion of HIPAA is complete without a prescription for compliance given by your friendly internal or external auditor, risk compliance officer or counsel. Unlike other recent federal legislation with security implications (such as the Sarbanes-Oxley Act, or "SOX"), however, HIPAA does not easily map to any "prescription" in the form of existing information security standards. SOX, for example, is premised upon a set of accounting standards known as COSO, and commentators have noted that the information security governance aspects of SOX can be mapped, in many respects, to a set of IT governance standards known as COBIT. Comments to the original and final drafts of the HIPAA Security Rule explicitly state that there is no "silver bullet" security standard for HIPAA compliance:

There is no recognized single standard that integrates all of the components of security... Therefore, we are designating a new, comprehensive standard, which defines the security requirements to be fulfilled. (Emphasis added).

And:

Since no comprehensive, scalable, and technology-neutral set of standards currently exists, we proposed to designate a new standard, which would define the security standards to be fulfilled.²⁰

¹⁹ For example, the Kaiser incident resulted in part from simple family animosity, but it ultimately had PR, legal and privacy repercussions for Kaiser.

²⁰ 68 *Federal Register* 8341.

To illustrate this point, HHS included “Addendum 3” to the proposed Security Rule, which cross-referenced existing information security standards to the rule’s standards. In its comments to the final Security Rule, HHS stated that “none of these standards was found to be comprehensive enough to be adopted, and none were proposed as the standards to be met under the Security Rule.”²¹

Because the Security Rule does not readily map to other existing standards, it may be easiest to understand the rule by breaking down its requirements into their three primary components: Administrative, technical and physical. The graph below illustrates this breakdown:

HIPAA Security Rule Standards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure(A) Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Healthcare Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control & Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)

²¹ 68 Federal Register 8345.

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic PHI (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

By breaking the rule down into these three basic categories, pathways to compliance begin to emerge. For example, the “CIA” standard (confidentiality, integrity, availability) stands as the goal of all implementation steps under HIPAA. Implementation efforts must focus on ensuring that electronic PHI is kept confidential, that its integrity (accuracy) is assured and that it is available when needed.

Like any good checkup, the process for checking HIPAA security compliance should begin with an initial evaluation by a process of risk analysis. First, the entity needs to determine whether it is a Covered Entity. Next, it must identify those systems, devices, processes and places within the company on or by which electronic PHI is created, received, transmitted or maintained. Because the Security Rule applies to electronic PHI however it is maintained (i.e., whether in transit, storage, on computers or on removable media), this may involve a review of workforce practices that do not, strictly speaking, relate to the network (for example, where and how backup tapes are stored).

After identifying the systems, devices, processes and places within the company on or by which electronic PHI is created, received, transmitted or maintained, the Covered Entity must evaluate its vital signs by engaging in risk management. It needs to determine which types of risks exist to the confidentiality, integrity and availability of electronic PHI, identify the source of these risks and then evaluate whether administrative, physical and technical safeguards exist to prevent such risks. A careful security evaluation should enable the Covered Entity to identify the existence and adequacy of existing security safeguards. Like blood pressure and temperature, these systems, devices, processes and places and the accompanying safeguards will change over time, so regular reevaluation of security “vital signs” and the ability to audit these changes is crucial.

After this process of risk analysis and risk management, the next step in the compliance process is to follow “doctor’s orders” and take the prescription for compliance by implementing safeguards. The Covered Entity must adopt the administrative, physical and technical policies, procedures and technologies needed to protect the confidentiality, integrity and availability of electronic PHI.

In this process, the simplest measures tend to involve physical safeguards. Measures as simple as locking rooms or file cabinets where PHI is stored on backup tapes can satisfy these measures. The more difficult implementation measures tend to involve administrative and technical safeguards.

Administrative measures are, in many respects, the “glue” that holds implementation efforts together. Although technical measures are often accomplished by help from vendors, the administrative measures sometimes end up being assigned to consultants who do not integrate their administrative solutions with the Covered Entity’s technical measures, or being handled internally by persons who may have little experience developing best practices and policies. The policies and procedures needed to meet the security specifications of HIPAA run the gamut of standard HR policies (termination and sanction policies) to more exotic security plans such as disaster recovery and emergency mode operation. Best practices references will enable institutions to prepare such policies and procedures based on the experience of others, rather than attempt to develop them from scratch. Furthermore, technical solutions that enable the Covered Entity to detect whether systems and even individual machines are being operated outside of policy parameters can assist in ongoing policy compliance efforts.

Because much of the PHI that must be controlled resides on computer systems, it is important that organizations have an independent, automated means to monitor their servers and workstations to ensure that inappropriate access and activities can be detected and dealt with in a timely fashion. As shown in the Kaiser example mentioned above, the ability to report on the activities of persons accessing PHI is crucial in mitigating risk of HIPAA violations.

The technical safeguards adopted by the Covered Entity must, at a minimum, be capable of detecting security incidents and protecting PHI. Because HIPAA focuses not only on confidentiality but also integrity and availability, however, the ability to restore the network to a known and trusted good state is required to restore PHI to its pre-exploit status and build an audit trail to comply with security incident reporting requirements. Technical solutions should also be able to detect unintended and malicious exploits and misuse from both inside and outside of the company network infrastructure, as the Kaiser example cited in this paper demonstrates.

Implementation of all of these administrative, physical and technical safeguards must be documented for a period of at least six years with clear, auditable proven records. Technical solutions that generate clear and easily understandable records of PHI use, and allow the Covered Entity to show a digital “paper trail” with regard to policy implementation, will go a long way toward satisfying this requirement.

In addition to these implementation steps, employee group health plans must comply with all of the above and also implement the technical and administrative means to protect electronic PHI as outlined in the plan sponsor requirements of the Privacy Rule. These requirements include adoption of administrative, physical and technical safeguards to maintain adequate separation of employee PHI from persons who could use the information for impermissible purposes (such as hiring or firing), procedures for the employer to report security incidents to the plan and amendment of the Health Plan’s plan document. The time-honored system of maintaining all employee records on a few unsecured computers in HR may have to change. As noted above, these requirements typically fall upon the employer as sponsor of the Health Plan due to practical (not legal) considerations.

Conclusion: Maintaining Network Health Through Independent Change Auditing

Last and certainly not least, changes to the Covered Entity's mindset concerning information security may be needed to maintain compliance with HIPAA's security provisions. Because the law, the security risks and the manner in which PHI itself is created, received, transmitted or maintained will all change over time, a simple "install and forget" approach will not meet HIPAA requirements. A process of ongoing change auditing is required to allow the Covered Entity to fulfill its statutory duties and avoid or mitigate civil lawsuits based on breach of medical privacy.

Change auditing involves combining technical solutions, administrative best practices and policies, assessment and review processes with top-level corporate decision-making into a seamless program. Incorporating information security, integrity and availability into the Covered Entity's standard business decision-making processes through a program of change auditing helps to guarantee that its security posture will have the flexibility needed to comply with compliance burdens today, tomorrow and beyond.

Adoption of an ongoing process of change auditing, as noted above, requires integration of all parts of the compliance process. Institutions may be best served by working with vendors that combine robust technical solutions which produce easily tailored and readable audit trails with complementary best practices resources to help Covered Entities meet the administrative and technical challenges of HIPAA compliance.

In the same way that a person's obligation to eat right and exercise regularly does not end after his or her annual physical, a Covered Entity's obligation to maintain HIPAA compliance does not end after the compliance deadline. If Covered Entities want to avoid an unannounced and potentially uncomfortable house call by the compliance doctor (HHS), then maintaining healthy systems, policies and procedures for PHI may be just what the doctor ordered.



Audit Change. Prove Control.

www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA

www.tripwire.com/intl/uk

TRIPWIRE UK: +44 207 618 6512 FAX: +44 207 618 8001
78 Cannon Street London EC4N 6NQ UK