White Paper: Rightsizing HIPAA Security Compliance

Abstract

The HIPAA security and privacy requirements are specifically designed using guidelines rather than hard and fast standards. These guidelines provide flexibility in scaling solutions for small to large organizations to address the law as well as to accommodate advances in technology. However, this very flexibility causes a quandary for smaller organizations because it’s unclear how far an organization can scale back and still meet the law’s requirements. This is particularly problematic in the security area where over 20 guidelines permit a wide range of interpretation.

This article addresses how much is enough and how to make defensible decisions in HIPAA implementation for healthcare organizations of all sizes. The law accounts for the fact that it is not possible to protect an organization from everything so the authors start with a discussion of how to determine what an organization should focus on. Then, it will cover specific recommendations for addressing security and privacy requirements based on these organizational-specific needs. It’s unclear how the government will enforce HIPAA standards because it hasn’t been tested in court but the goal of this article is to bring to the forefront information on implementing sound security practices which, according to the law’s authors, was the intention in the first place. The authors of this article will focus on real-world experiences.

This paper is currently under peer review for publication in the summer 2003 issue of the Journal of Health Information Management. All rights reserved.

The opinions, descriptions, and recommendations herein are intended as an aid to assist you with understanding the HIPAA security rule, and cannot nor should not be construed as legal advice.
There Is No Privacy Without Security

The Department of Health and Human Services estimates that there are 200,000 small health care providers (less than five physicians) considered “Covered Entities” under HIPAA legislation. These organizations must address HIPAA requirements by the deadline or risk suspension of payment, expulsion from Medicare, and other significant penalties. Most organizations are familiar with the privacy rule and requirements since the timeframe for compliance required their attention first. However, many organizations have not devoted sufficient time to security requirements and fail to realize that there can be no privacy without security. The law recognizes that security and privacy are strongly linked and has addressed it in the final security rule, published February 20, 2003.[1]

The final security rule outlines 18 standards covering 36 implementation specifications protecting the confidentiality, integrity, and availability of individually identifiable health information. This standard was developed to be flexible to take advantage of maturing industry “best practices,” scalable so that it could be used effectively with organizations of all sizes, and technology neutral so that future technologies could be used without changing the standard. Smaller organizations with limited resources and simpler networks will need to do less to ensure compliance than large organizations with very complicated infrastructures. So organizations are left with the problem of rightsizing their security practices to fit HIPAA compliance. How much security is enough?

Building flexibility into a standard may be the right thing to do but it’s not trivial. Many people have expressed concern over meeting a standard that has so much flexibility built-in that it will not be a standard at all. The final rule uses both “required” and “addressable” implementation specifications in an attempt to build clarity into the flexible aspects of the rule. Required specifications are things you must do. Addressable specifications are required if it is “reasonable and appropriate” to apply the specifications within an organization’s particular security framework. Independent of the implementation, you must meet the standard in all cases.

Although some of the implementation specifications are addressable, that does not mean they are optional. This decision of appropriateness is left up to the organization, but the rule does give guidelines including using the risk analysis process, risk mitigation strategy, security measures already in place, and the cost of implementation to use as factors in making the decision. This should not be interpreted as license to say “well, it was too costly, so we didn’t do it.” The law goes on to say that if you choose not to implement an addressable specification then you have to implement an alternate measure. In the event that you decide you can’t implement an alternate measure either, then you must document the decision, the rationale, and how the standard is being met.

Even the required specifications do not have rigidly defined implementation directions. There are some basic concepts that will help you set the appropriate level of security. Some of these are based on industry best practices. Others take advantage of the flexible manner in which the standards are presented. However, this flexibility is a double-edged sword and should be used with care. Always document your decisions so that you can have a defensible position if your compliance is ever questioned.

Things you can do to “rightsize” HIPAA security compliance and lower your overall risk:

- Complete a self-certification with third-party review of your compliance.
- Perform a risk analysis, understand residual risk, and don’t try to protect yourself from everything.
- Exercise due care and due diligence to meet the standard of due care.
- Use technologies appropriate to your organization.
The Security Rule

The security rule (see Figure 1) recognizes that every organization is unique and will have unique requirements. The rule was developed with the following design goals in mind:

Comprehensive. It had to effectively safeguard protected health information (PHI) across many different types of organizations with radically different operational modes including health plans, providers, and insurance companies.

Technology neutral. The standard could not reference or advocate specific technology because security technology is changing quickly. Covered entities need the flexibility to choose their own technical solutions. A standard that is dependent on a specific technology or technologies would not be flexible enough to use future advances.

Scalable. It had to work for the smallest organization and the largest. A single approach with fixed requirements would be neither economically feasible nor effective.

The National Research Council’s 1997 report, “For The Record,” recommended “All organizations that handle patient-identifiable health care information—regardless of size—should adopt the set of technical and organizational policies, practices, and procedures described below to protect such information.” [2]

As a result of the collaborative security regulation development process, the implementation team chose to divide the proposed security requirements into the following categories:

Administrative Safeguards. These are documented practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.

Figure 1: The Elements of the HIPAA Security Rule
Physical Safeguards. These relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

Technical Safeguards. These are processes to protect, control, and monitor information access. These include the processes that to prevent unauthorized access to data that is transmitted over a communications network.

When rightsizing your compliance plan you can use the lack of specificity in the rule to make choices that are appropriate and fit within your budget. However, be prepared to defend each decision you make.

Don’t Protect Yourself from Everything: Understanding Residual Risk

One of the core tenets of information security is that you can’t protect yourself from everything. The final comment on the rule signed by HHS Secretary Tommy Thompson states “We agree…that there is no such thing as a totally secure system that carries no risks to security.” It goes on to add “…we intend that a covered entity take steps, to the best of its ability, to protect [the safety of information in its keeping].” You need to perform a risk analysis to determine the threats that are most applicable to your organization and protect yourself from those threats.

Risk is usually mitigated with the use of protection measures, or transferred to a third party through mechanisms like insurance. What remains (risk that is neither mitigated nor transferred) is known as “residual risk” and this must be accepted. Acceptance means understanding what known risks the organization is not protected against and what to do if one of these risk scenarios causes a loss. Residual risk becomes part of your operating plan.

When rightsizing HIPAA compliance you should not try to protect yourself from everything. This can help you stretch limited resources to make the most of your information security. However, you need to understand what you aren’t protected from (residual risk) and have a contingency plan if something happens.

The Standard of Due Care

The rule says that enforcement will be addressed in a later rule. Although there are no HIPAA “police” at this time, and the requirements are defined in such a way that it is difficult to determine exactly what comprises compliance, there are some time-tested techniques to determine if an organization is in compliance. The standard of due care is a subjective standard used to grade an organization’s compliance by measuring it against its peers.

Healthcare providers today need to protect themselves by exercising due care and due diligence. Due care means that you did all you could to reasonably protect your organization from known threats. Due diligence means that you kept up with these practices in a diligent manner, rather doing them once and then forgetting about them.

Senior management is responsible for protecting the organization from a long list of actions that can have a negative impact including protecting personal privacy, leaving the organization open to hacker attack, malicious code, and violation of the law. Management must follow the “prudent person” rule which requires them to perform duties that prudent people would follow in similar circumstances using due care and due diligence.

In practice (in a court of law), due care and due diligence are subjective and usually defined by what other companies are doing and what a prudent management team would do. In other words, if most other companies are doing third party audits to check their own security measures and you have not done one, then you could be held liable for not having taken prudent and reasonable actions to prevent misuse.
On the other hand, if you have done reasonable and prudent things such as a third-party audit, then, even if your machines were misused resulting in a compromise of PHI, you have some protection against liability. At the very least these actions would count in your favor.

Unfortunately, determining what your peers are doing can be a challenge. You can use conferences and other professional meetings to gather anecdotal evidence of what other organizations are doing. You can also read journals and other publications to identify trends. In practice, the standard of due care is interpreted on a case-by-case basis during a trial so it’s very subjective. All you can really do is stay educated and use your best efforts to maintain parity with your peers.

Self-Certification and Third-Party Review

At this time, there are no specific organizations authorized to perform certifications. However, HHS recommends a self-certification to meet the requirements of the HIPAA security rule. Self-certification must:

- be performed by individuals who are not responsible for the maintenance, supervision, or execution of the specified IT controls;
- be an on-going process;
- include due diligence as a requirement;
- include documentation as a key part of the process;
- be performed by individuals with adequate training regarding generally accepted security guidelines and principles;
- be performed by internal or external parties;
- include an examination of evidential matter sufficient to obtain an understanding of the design and effectiveness of controls for each HIPAA security requirement and implementation;
- recommend monitoring the certification cycle at a minimum of once a year due to the changing nature of computer systems and accelerating rate of change of IT related security risks;
- be maintained for three years to provide for an adequate history of certification information and an audit trail of certification for reviewing bodies;
- be reviewed and authorized by executive management.

Although the recommendations suggest that an internal party may do self-certification work, this internal party would also need to have adequate training and be individuals who are not responsible for the maintenance, supervision, or execution of the specified IT controls. Typically, when small organizations have someone with the proper training these are the same individuals responsible for the management of the systems being certified. Objectivity is crucial to the validity of the self-certification. The law does not require external review but it could count against you in any enforcement action if the standard of due care indicates that most organizations are using external review.

This self-certification is documented in a letter in management representation form signed by the organization’s executive management and compliance officer that states 1) the compliance status by each HIPAA requirement and element, 2) management’s action plans to address areas of control deficiency, and 3) any instances in which management is aware of security related control issues or deficiencies. This letter clearly states management's responsibility for the effectiveness of the information security control structure.
Examples of Rightsizing HIPAA Compliance

The following are real-world examples of how organizations have created reasonable plans to comply with seven of the HIPAA security standards using limited resources.

**Contingency Planning 164.308(a)(7)**

Requirement: A contingency plan is required to be in effect for responding to system emergencies. The organization is required to perform periodic backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place.

Compliance: This is one of the original examples used in the Notice of Proposed Rule Making (NPRM)[7] where it states. “For example, in a small physician practice, a contingency plan for system emergencies might be only a few pages long, and cover issues such as where backup diskettes must be stored, and the location of a backup personal computer (PC). At a large health plan, the contingency plan might consist of multiple volumes, and cover issues such as remote hot site operations and secure off-site storage of electronic media.”

**Access Control 164.312(a)(1)**

Requirement: Access control restricts access to resources and allows access only by privileged entities. It is important to limit access to health information to those employees who have a business need to access it.

Compliance: A larger organization with hundreds of employees may determine that it needs to adopt a formal policy for access authorization. In smaller organizations, all that is necessary is to put the PHI on servers that can only be accessed by authorized personnel with a password. The most significant change is that PHI must be centralized and controlled, so there can be no more open-shares on the network and no more PHI on desktops and shared machines.

**Encryption 164.312(a)(1)**

Requirement: Encryption is a mechanism to protect PHI from unauthorized disclosure. This refers to encryption for stored data rather than transmitted data that is covered in 164.312(e)(1). This is an addressable specification so you need to make a decision about its appropriateness in your environment.

Compliance: If your risk analysis shows that you are at significant risk of unauthorized access, then encrypting PHI on your desktop may be necessary. If it is not a significant risk, then you can choose to keep your files in clear text readable format and accept the residual risk of someone gaining unauthorized access and reading or stealing you PHI. You should have a contingency plan to handle this situation if it arises.

If your compliance is called into question because your files are not encrypted, the court (or other enforcement agency) will likely turn to the standard of due care for an indication. Are other organizations in similar businesses, with similar sizes, encrypting their files? If not, then you have a case for doing what was prudent in your position. If everyone else is encrypting and you are not, then you may need to prepare for some heavy fines.

**Workforce Security 164.308(a)(3)**

Requirement: All personnel with access to health information must be authorized to do so after receiving appropriate permission.

Compliance: In larger organizations, with many levels of access and types of PHI used for different reasons, the controls to enforce personnel security can include whole managed departments of human resources people managing who has access to what, the clearance procedures, and the records.
smaller organizations it can be as simple as separating the privileges of those who require PHI and those who don’t. Then, assign an individual to authorize and grant access to people. If you have the resources, you can assign the role of authorizing access to a different person who grants access providing a small, but effective implementation of the “two-person” rule. This is a very inexpensive way to reduce risks.

**Security Awareness and Training 164.308(a)(5)**

Requirement: Security training is required for all staff regarding the vulnerabilities of the health information in an entity’s possession and procedures that must be followed to ensure the protection of that information.

Compliance: Security training is simpler in smaller organizations because there are fewer offices, fewer departments, and fewer procedures. Training can be accomplished at a company-sponsored lunch because the basics are the most important and don’t take that long to convey and test understanding. These include: What is PHI? Am I allowed to possess PHI? How do I protect PHI? What do I do if I observe PHI being compromised or at risk of being compromised? You should also make sure every employee reads the company processes and procedures manual for HIPAA and signs a form stating their understanding and compliance.

**Facility Access Controls 164.310(a)(1)**

Requirement: Physical access controls (limited access) are required. These are documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed.

Compliance: In smaller organizations, where everyone knows each other, it is a lot easier to implement physical access. It isn’t necessary to have proximity key cards and badges. Procedures need only specify that doors are locked when an unauthorized person is not present. PHI should be kept in one place where access can be monitored. This is one area where HIPAA requirements are changing the way many offices do business by restricting casual handling of PHI.

**Integrity 164.312(c) (1)**

Requirement: This addressable implementation specification provides corroboration that data in its possession has not been altered or destroyed in an unauthorized manner.

Compliance: In most cases, your software application provider will handle anything you do electronically that would be covered by this requirement for electronic data interchange like billing. Although this is an addressable specification, this an area where there are some simple things you can do that don’t cost a lot. Using a personal certificate, available from providers like VeriSign, that is embedded in your email and browser programs will be sufficient to meet this standard and the transmission security standard 164.312(e)(1).

**Conclusions About “Rightsizing” HIPAA**

There is no privacy without security. Many organizations are concerned about the cost associated with meeting the requirements in the HIPAA security rule because they don’t know how much security is enough and the law doesn’t provide enough guidance. However, if you do the following then the security rule can be tamed:

- choose controls appropriate to your organization;
- do a risk assessment to determine appropriate risks;
- understand and have a plan for your residual risks;
• compare your choices to what everyone else is doing;
• exercise due care by doing it right the first time;
• exercise due diligence by continuing to review and update your security;
• get third-party review of your compliance.

Case Study

Strategic Healthcare Programs, LLC, based in Santa Barbara, California, is a healthcare technology company specializing in products and services that deliver clinical and business intelligence data to home healthcare providers. SHP has 1200 clients nationwide and serves as a business associate to its customers, all of whom are covered entities. SHP is required to comply with HIPAA mandates to secure the privacy and confidentiality of the PHI it receives from its clients.

SHP is a relatively small organization with two offices. The company’s database contents are its main business asset and the protection of data is paramount not only for purposes of complying with HIPAA, but from a business perspective as well.

SHP took what it believed to be reasonable steps to protect the confidentiality of its customers and the patient data to which it was entrusted. When HIPAA standards were released, the company was confident that it understood and complied fully with privacy regulations. However, after performing its own security gap analysis using a publicly available checklist, the company felt it prudent to engage the services of a security specialist.

Barbara Rosenblum, CEO of SHP and Chairman of the HIPAA compliance committee, made the decision to outsource security help to comply with the HIPAA requirements. Rosenblum said, “I don’t resent the mandates from HIPAA. I believe they have encouraged us to adopt practices that are in our best interest from a business perspective.”

SHP assembled a HIPAA Committee comprised of key members of the organization’s departments. The first few meetings were extremely lengthy as the company tried to gain an understanding of the requirements and their intent, and determine which mandates were already met and which required attention. Subsequent meetings focused on the unmet mandates, which quickly led to the realization that the company needed help to both identify areas of security risk and to develop a plan of remedial action.

Once the decision was made to have an outside firm perform a security audit, the next tasks were to identify all of the places on the network where Protected Health Information (PHI) existed. Then, they needed to diagram the network in such a way that would make it easy for an outside firm to come in and quickly understand SHP’s infrastructure and business model.

Nick Davis, Director of Information Technology, says, “We knew that we had some areas of our network that we could improve, but systematically looking at each piece, and describing the potential risks to the security consultants really helped us quantify exactly what needed to be done.”

SHP’s security audit took about three days. Several staff members, from the receptionist to the CEO were interviewed to gather information on their roles, responsibilities, and general access to PHI.

Several key findings came out of the interview process. Don Taylor, Vice President of Product Development, was concerned that he would no longer be able to demonstrate certain aspects of SHP’s programs that contained PHI after April 2003. He was reassured to learn that if a simple Business Associate Agreement could be executed between the prospect and SHP, then demonstrations that contain the prospect’s PHI could continue after the HIPAA deadlines.

Many of the findings in the security audit focused on the need to separate PHI from non-PHI on the network, and to assign access rights to these areas of the network to staff members accordingly, based on their roles and responsibilities. Nick Davis remembers, “because we had already identified all the

www.practicalsecurity.com 8 of 8 3/10/2003
places where PHI resided, the task of actually separating the PHI and assigning group-level access to those places was not that difficult. Within a few days, we had many of the places with PHI effectively locked down.”

Other recommendations made by the security consultants were not so easy to implement. “We were advised to set up a DMZ (Demilitarized Zone), but didn’t have a test network to experiment with, so there was some impact to our production network while we figured things out” said Davis.

Davis offers this insight to small and medium-sized organizations: “Get help with the security portion of HIPAA. Privacy regulations are easily understood, but security is its own specialty. Remember that there is no privacy without security. Protect the investment you’ve already made in complying with privacy. Stifle any temptation to believe that you can do it all yourself. Recognize that you might end up spending time and money to over-comply, not to mention the risk that comes with under-complying.”

Not all of the areas of risk identified in the audit process could be addressed. There were areas of risk that were too expensive or too difficult to address. The executive staff and the HIPAA compliance committee had to determine the likelihood of a breach in those areas, and the repercussions. It was decided that some amount of risk was acceptable, especially if the scenarios have been discussed and contingency plans have been drawn up.

There is much a Covered Entity or Business Associate can do to lock down the PHI on their networks, without a huge investment in time or money. SHP identified the tasks that gave the biggest return on investment and focused on them. Increasing awareness of PHI to all staff members, separating PHI from non-PHI on the network, and locking down those parts of the network that have PHI were the most significant steps taken by SHP to achieve compliance.

Author’s Note: The final security rule was adopted 2 days before this paper was due for publication. Originally based on the Notice of Proposed Rule Making (NPRM), it required significant analysis and rewrite in that short time. It does not include any public comment or analysis in the months following release of the final rule.

Author Biographies

**Paul E. Proctor**

Mr. Proctor is President and CTO of Practical Security, Inc. ([www.practicalsecurity.com](http://www.practicalsecurity.com)) He has over 17 years experience in computer security, and helps organizations meet these requirements in the real world. Mr. Proctor can be reached by email at mailto:peproctor@practicalsecurity.com?subject=HIPAA Security White Paper.

**Nick Davis**

Mr. Davis is director of IT at Strategic Healthcare Programs, an information analysis firm that recently tackled the challenges of HIPAA compliance in a smaller organization.

**Barbara Rosenblum**

Ms. Rosenblum is founder and CEO of Strategic Healthcare Programs. As author and winner of the 1997 National Managed HealthCare Organization's HITS Award, she is recognized as a healthcare leader.
References


