

# HIPAA SECURITY

## Made Simple

for Physician Practices

Practical Compliance  
Advice for Small Offices

Kate Borten, CISSP, CISM

Made Simple

# Contents

<b>About the Author</b> .....	<b>vii</b>
<b>Chapter One: HIPAA Security Introduction and Overview</b> .....	<b>1</b>
What is HIPAA? .....	3
How security fits in .....	4
How to use this book .....	6
Compliance Step 1: Understand the security rule .....	7
Compliance Step 2: Appoint an information security officer .....	7
Compliance Step 3: Risk assessment .....	7
Compliance Step 4: Develop your security program .....	8
Layered approach .....	10
Pitfalls to avoid .....	10
Documentation tips .....	12
<b>Chapter Two: HIPAA Security Rule: General Rules</b> .....	<b>15</b>
General requirements .....	18
Flexibility of approach .....	20
Standards .....	21
Implementation specifications .....	22
Maintenance .....	24
<b>Chapter Three: HIPAA Security Rule: Administrative Safeguards</b> .....	<b>25</b>
Security management process .....	28
Risk analysis .....	30
Risk management .....	34
Sanction policy .....	41
Information system activity review .....	44
Assigned security responsibility .....	46

## Contents

Workforce security . . . . .	48
Authorization/supervision . . . . .	49
Workforce clearance procedure . . . . .	51
Termination procedures. . . . .	53
Information access management . . . . .	55
Isolating healthcare clearinghouse function. . . . .	56
Access authorization . . . . .	57
Access establishment and modification . . . . .	61
Security awareness and training . . . . .	67
Security reminders. . . . .	72
Protection from malicious software . . . . .	73
Log-in monitoring . . . . .	74
Password management . . . . .	75
Security incident procedures . . . . .	78
Response and reporting. . . . .	78
Contingency plan . . . . .	83
Data backup plan . . . . .	84
Disaster recovery plan. . . . .	86
Emergency mode operation plan . . . . .	89
Testing and revision procedures . . . . .	90
Applications and data criticality analysis. . . . .	91
Evaluation . . . . .	93
Business associate contracts and other arrangements . . . . .	95
Written contract or other arrangement . . . . .	96

## **Chapter Four: HIPAA Security Rule: Physical Safeguards . . . . . 97**

Facility access controls . . . . .	100
Contingency operations. . . . .	101
Facility security plan . . . . .	102
Access control and validation procedures . . . . .	106
Maintenance records. . . . .	108
Workstation use. . . . .	109
Workstation security . . . . .	114
Device and media controls . . . . .	116
Disposal . . . . .	117

Media re-use . . . . . 119  
 Accountability . . . . . 120  
 Data backup and storage . . . . . 123

**Chapter Five: HIPAA Security Rule: Technical Safeguards . . . . . 125**

Access control . . . . . 127  
 Unique user identification . . . . . 129  
 Emergency access procedures . . . . . 131  
 Automatic log off. . . . . 132  
 Encryption and decryption . . . . . 134  
 Audit controls . . . . . 136  
 Integrity . . . . . 141  
 Mechanism to authenticate electronic protected health information . . . . . 141  
 Person or entity authentication . . . . . 143  
 Transmission security . . . . . 146  
 Integrity controls . . . . . 147  
 Encryption . . . . . 148

**Chapter Six: HIPAA Security Rule: Additional Organizational Requirements . . . 153**

Business associate contracts or other arrangements . . . . . 155  
 Business associate contracts . . . . . 156  
 Other arrangements . . . . . 157  
 Requirements for group health plans . . . . . 158  
 Group health plans . . . . . 158  
 Policies and procedures and documentation requirements . . . . . 159  
 Policies and procedures . . . . . 159  
 Documentation . . . . . 159  
 Time limit . . . . . 160  
 Availability . . . . . 160  
 Updates . . . . . 160

## Contents

<b>Chapter Seven: HIPAA and Security of Nonelectronic PHI</b> .....	<b>161</b>
Oral disclosure of PHI .....	164
Faxed disclosure of PHI .....	165
Protecting other paper PHI .....	167
A clean-desk policy .....	168
Disposing of paper and other non-electronic media safely .....	168
Administrative controls .....	169
<b>HIPAA Security Rule: Appendices</b> .....	<b>171</b>
Appendix A: HIPAA Security Rule, Security Standards: Matrix .....	173
Appendix B: Resources .....	177
Appendix C: Standard password controls .....	179
Appendix D: Sample job description for information security officer in a small office .....	181
Appendix E: HIPAA security points to consider in small offices .....	183
<b>How to use the files on your <i>HIPAA Security Made Simple for Physician Practices</i> CD-ROM</b> .....	<b>187</b>
<b>Related Products from HCPPro</b> .....	<b>189</b>

**CHAPTER ONE**

**HIPAA  
SECURITY  
INTRODUCTION  
AND OVERVIEW**

# HIPAA Security Introduction and Overview

## What is HIPAA?

When Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it included a major section entitled Administrative Simplification. This section requires the health-care industry to streamline and simplify computer processing of electronic transactions—primarily between providers and payers, involving claims, payments, and eligibility checking. As part of this effort, it mandates standardized record formats and code sets for those transactions. This will result in less customized processing for each different payer and, thus, lower processing and software support costs to the industry, possibly leading to faster turnaround time on claims submission and payment.

Congress anticipated that the healthcare industry would eventually process most (if not all) of these transactions electronically. As the healthcare industry's external business transactions become increasingly electronic, the risks to patient privacy and security of information also increase. Hence, Congress included in Administrative Simplification two new sets of regulations to protect that data.

These two sets of regulations included a privacy rule and a security rule, both of which Administrative Simplification directed the U.S. Department of Health and Human Services (HHS) to develop. On April 14, 2003, the privacy rule became an enforceable set of regulations. In February of 2003, HHS released a final security rule and, as with the privacy rule, provider organizations subject to it ("covered entities") have 24 months, or until April 21, 2005, until the security rule becomes enforceable. That is, however, an artificial deadline because, based on existing privacy rule requirements, providers already should have a security program in place.

## Chapter One

Administrative Simplification defines “covered entities” as all health plans, healthcare clearinghouses, and healthcare providers that engage in certain electronic transactions. That definition generally omits providers who do not submit insurance claims or who submit all claims on paper (i.e., typically only nontraditional or very small provider organizations). If you need help determining whether your organization is a covered entity, see the HHS Centers for Medicare & Medicaid Services (CMS) Web site ([www.cms.hhs.gov](http://www.cms.hhs.gov)) and type “covered entity” in the search window to access its decision-support tool.

Although HIPAA does not define different types and sizes of provider organizations, this book is primarily directed toward small healthcare provider organizations, which are characterized as those with a

- single physical facility
- single primary software application vendor (excluding desktop software, such as Microsoft Office)
- small, simple local network using a single network operating system (e.g., Windows NT or Novell), with limited access to and use of the Internet and other large networks

Examples of such facilities include small physician practices, dental and vision offices, and ambulatory physical therapy clinics. This book can also be helpful for small businesses, such as transcription and billing offices, which are not covered entities themselves, but are business associates of covered entities.

### How security fits in

The concepts of privacy and security are closely related. The first, information privacy, addresses each individual’s right to control his or her personal information. Privacy laws spell out the conditions under which organizations may use personal information and the obligations of organizations to protect such data. HIPAA’s privacy rule specifies when a covered physician practice may use protected health information (PHI)—essentially, any information about a patient that can be tied to that patient—with and without that patient’s permission.

The second concept, information security, addresses the confidentiality, integrity, and availability of PHI. Confidentiality means that only authorized individuals, with a legitimate work-related

need, have access to PHI. Integrity means that the PHI can be trusted, and that it has not been tampered with or otherwise inappropriately altered. Availability means that authorized individuals or computer processes are able to access PHI when they need to.

HIPAA's privacy rule requires that covered entities ensure these three aspects of security, by using administrative, physical, and technical safeguards (security measures), to protect PHI in all forms (oral, written, and electronic). In this way, HIPAA intertwines privacy and security.

However, because the impetus for this rule came from the Administrative Simplification focus on electronic transactions, the security rule only applies to PHI in electronic form (ePHI), a subset of the PHI that is specifically protected under both the original HIPAA law and the privacy rule. Although it is clear that organizations must take steps to protect all PHI, organizations are confused about how to do it—and about which security protections must be in place now and which are not due until 2005.

Regardless of technical due dates, most legal experts and information security professionals say now is the time to address security protections for all PHI. There is enough overlap between the two rules that if a security breach led to significant consequences, HIPAA penalties under the privacy rule could be imposed today. Further, enforcement actions from other government agencies (e.g., the Federal Trade Commission), private lawsuits, and negative publicity will not wait for the artificial deadline of 2005.

Therefore, covered entities have no reason to delay addressing security. Administrative security mechanisms, security resources, and best-practice principles are readily available to those who seek them. The healthcare industry has lagged behind other sectors in recognizing the need for formal information security programs, and it will now need to catch up.

Physician practices should recognize the importance of security and understand that it is not a one-time compliance project. Security will continue to evolve as new risks arise, as business practices develop, and as HHS modifies its baseline standards. The government reserves the right to make annual changes once rules are in force, and security experts expect it to use this right. Therefore, physician practices should view their security efforts in that light, rather than as a race to the finish line.

## Chapter One

HHS has stated that it will not be an accrediting body and that it does not intend to routinely review covered entities' compliance. However, if a complaint is filed with the Secretary of HHS, there will be enforcement processes in place. Administrative Simplification provides both civil and criminal penalties:

- civil penalties are for noncompliance with the Administrative Simplification rules
- criminal penalties are broadly for "wrongful disclosure" of PHI, with increasing fines and prison time depending on the intent behind the wrongful disclosure

Although the privacy rule enforcement occurs within HHS's Office for Civil Rights (OCR), security issues and rule enforcement fall under HHS's CMS division in the Office of HIPAA Standards. HHS criminal complaints are turned over to the Department of Justice.

Although HHS authority is limited to covered entities, organizations such as physician practices must impose contractual limits and obligations on their business associates (i.e., third parties with access to a covered entity's PHI) who are performing work on behalf of the covered entity. A covered entity must require its business associates to protect PHI and only use and disclose PHI in accordance with the limits of the contract between the two parties, and not in a way that would be prohibited by the privacy rule.

### How to use this book

This book will explain the security rule in detail and provide practical guidance to small physician practice offices for complying with the rule. View a complete copy of the security rule and preamble, along with all the sample forms in this book, on the accompanying CD-ROM.

The rule is comprised of "standards" and "implementation specifications," both of which are defined in Chapter Two. Throughout this book, standards and their underlying implementation specifications are clearly identified with the rule's exact language and section reference. Each standard and specification is followed by a discussion of its background and intent, which are taken from the rule's preamble and, in some cases, from the proposed security rule of 1998 and other supporting documents. Each is also followed by practical tips on compliance.

### ***Compliance Step 1: Understand the security rule***

When you gain a thorough understanding of the rule and its implications for your office, you take an important first step toward compliance.

Note that the rule does not specify how an organization should meet each requirement. Because healthcare organizations vary widely in size, complexity, technologies, and resources, the rule provides wide flexibility in how you may comply with it. This flexibility makes compliance easier, but it also means that organizations have significant responsibility for understanding and living up to the intent of the rule. For physician practices just getting started with security, there are no black-and-white answers.

### ***Compliance Step 2: Appoint an information security officer***

Appoint an information security officer (ISO) who will take the lead in establishing the program and have ongoing responsibility for it. If you have not yet established a security program, read this book before you do to fully appreciate the scope and skills necessary for the person who fills that critical role. Although information security involves technology, there is much more to the ISO position than information technology (IT) knowledge. In a small office, this position is likely to be a part-time role taken on by a person with limited technical expertise and other major duties (similar to the privacy officer role in a typical office setting). Chapter Three includes further discussion on this position.

### ***Compliance Step 3: Risk assessment***

Once your designated ISO is well-versed in the security rule, he or she should begin assessing your organization's current risk. Whether your organization intends to set the gold standard for your peers or expects a challenge in meeting even basic requirements, the rule requires that each organization evaluate its own particular risks and take steps to mitigate them.

The following are two types of risk:

- Risk of noncompliance with HIPAA regulations and other laws
- Security risks to confidentiality, availability, or integrity of information

In general, if you are in compliance with regulations, you are expected to address security risk. Addressing risk does not mean you have eliminated it. Risk is dynamic, and there is always some risk to your information. Thus, all organizations should have mechanisms in place to monitor

## Chapter One

their risk. Both the rule and good security principles require you to have dynamic processes that prevent, detect, contain, and correct security breaches.

After reading this book, you may worry that the work is overwhelming. But a comprehensive risk assessment, which the rule requires, will give you an overview of your situation and spell out which risks are a high priority, as well as those that can be addressed easily and promptly. This assessment creates a blueprint for compliance work and sets the stage for planning the tasks, deciding who will perform them, and determining what to budget. More information on the assessment process can be found in Chapter Three.

### ***Compliance Step 4: Develop your security program***

The assessment and project-planning phase will set you on the road to compliance. It will also help you determine which security measures should be currently in place and which measures can be delayed. By initiating security planning and addressing high risks now, your practice will be less likely to experience a security breach, and it will be in a better position to handle a legal challenge.

Some risks call for technical solutions that may not be available to you. For example, your software vendor may not provide certain features yet, and other products may be beyond your budget this year. (*Note: Omitting security controls or technologies simply because they cost money is not acceptable. However, a product's cost should be appropriate for its benefit in risk reduction.*) You may choose to mitigate certain risks through compensating controls until you can address them in a more robust manner. For example, if your software has weak password-management features, but your vendor has promised to provide an upgrade next year, you may focus on procedures and workforce training to compensate in the interim for that software shortcoming. Document such decisions and compensating measures.

Figure 1.1

**Quick Start to Compliance**

***Compliance Step 1: Understand the security rule and information security***

Take time to read the rule, including its preamble. Seek out additional resources, such as books, audioconferences, seminars, and Web sites, to learn as much as possible about information security and formal information security program principles and components. Continue to expand your knowledge on an ongoing basis.

***Compliance Step 2: Appoint your information security officer***

Designate one person to become “security smart” and to lead your security rule compliance effort. (See Chapter Three for more information about this role and desirable characteristics for the individual who fills it.)

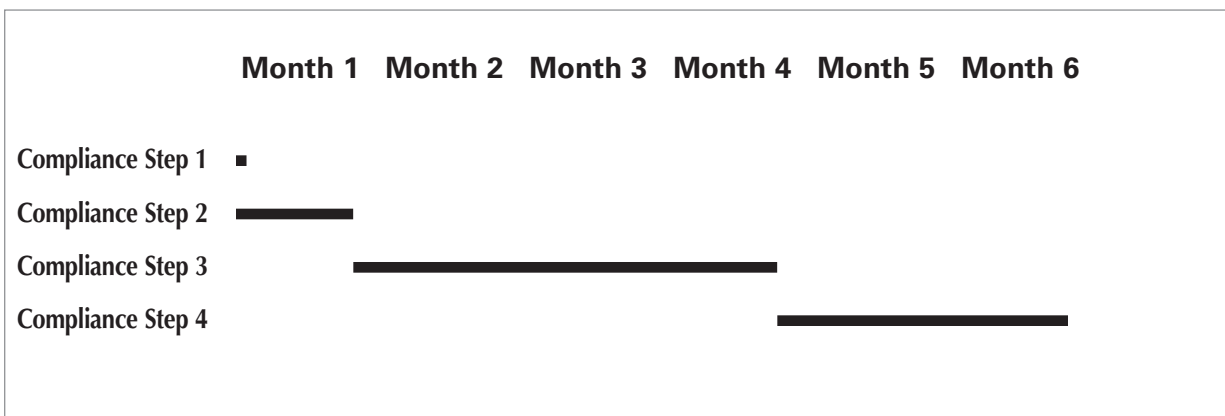
***Compliance Step 3: Perform your initial risk assessment***

Decide whether you can do this on your own or whether you will seek outside help. Determine what tools and methodology you will use or what approach you will take to perform a reliable, comprehensive assessment. After completing the assessment, review the resulting observations (identified risks) and recommendations with your management. Plan and begin work to address them.

***Compliance Step 4: Develop your security program***

If you are building your security program from the beginning, the outcome of Step 3 should be a project work plan for both addressing the risks you have found and for building the components of a sound information security program, as required by HIPAA.

Here are approximate timelines for the above compliance steps. They indicate the relative amount of time each step is likely to take. Actual time will vary for each organization.



### Layered approach

There is always some risk—it's just a matter of degree. You don't normally eliminate risk through security measures; you lessen or mitigate it to an acceptable level for your organization. Security risks are everywhere: in technology, in staff behavior, and in the physical environment. Thus, security solutions come in many forms. Security professionals describe them as layers or strategies, with each contributing to the overall security environment. The following approach to access control illustrates an example of layered solutions.

Ensure that only authorized individuals have access to PHI. (*Note: Access control is relative, not absolute. Even if you take reasonable measures, there may still be a way for someone to “break in” and gain access.*) In an electronic environment, that goal is typically achieved through a variety of administrative, physical, and technical mechanisms that might include the following elements or layers:

- Use of firewalls
- Adherence to server-configuration standards
- Adoption and use of change control procedures
- Locking data centers and server rooms
- User authorization policies and procedures
- Workforce training about password management

In this layered approach, certain controls complement those that are deficient to provide a reasonable and appropriate level of security. For example, if your vendor application-level security features are weak, you may decide to compensate by more fully employing operating system-level controls and providing enhanced user training.

### Pitfalls to avoid

Once you learn what the security rule requires, assign someone to lead the security program, but be aware of the following common pitfalls:

- Avoid the urge to solve known security problems immediately. Sometimes it's better to wait until you have a complete assessment before taking action. You may find that solutions are interdependent or you may decide that other security issues are more urgent and deserve a higher priority based on staff or budget resources. By prematurely creating a procedure to resolve one problem, you may miss an opportunity to take a better approach that solves several.
- Avoid focusing exclusively—or even primarily—on technology. Much (if not most) of security is administrative work, e.g., policies, standards, procedures, and training.
- Avoid letting technology dictate policy. Ideally, set policy first—with available technology solutions in mind—and then implement the supporting procedures and technologies to fit the policy.
- Avoid buying either the wrong technology or too much technology. Sometimes vendor hype and technical gadgetry create a strong pull. Be sure you understand the problem to be solved, and thoroughly investigate its impact and your options before investing in new security technologies. Any technology you select should be the best solution for your particular problem in your particular risk environment, keeping in mind your resources.
- Avoid underestimating the time and knowledge needed to achieve reasonable security. Your ISO will need to take time to learn about information security principles and requirements of the security rule, as well as to develop and implement ongoing security processes. Others in the office also will need to take time periodically for security related tasks.

Notice that most of the above suggestions rein in technology spending. Healthcare organizations on tight budgets can often achieve reasonable security without purchasing the latest technology. Administrative controls, such as following procedures and providing workforce training, are largely technology independent and basic security technologies (e.g., embedded password controls, firewalls, anti-virus software) have become less expensive and more readily available.

### Documentation tips

The following are several general policy-and-procedure compliance tips to keep in mind:

- Organizations sometimes neglect to document policies and procedures. But besides being required by the rule, clear and current documentation has true value that
  - forces you to review processes that uncover gaps and inconsistencies, for which you can design new solutions or protective countermeasures
  - ensures that everyone understands the organization's expectations
  - ensures consistency (i.e., everyone performs the same process in the same manner)
  - provides invaluable training tools for new members of the workforce
- In a small healthcare organization, such as a small office practice, a policy and its related procedures may be combined into a single document called a standard operating procedure (SOP). Such a document is typically brief and combines a policy goal with specific procedures. The content of the SOP is important, and it must be documented and followed by your workforce.
- When the security rule requires a policy, start by paraphrasing the rule. For example, the following is a sample policy statement, using rule language that would satisfy the policy requirement of the Contingency Plan standard and its underlying specifications:

*"This organization shall have an overall contingency plan and supporting procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information and other confidential and proprietary data. This plan will include procedures for data backup, procedures for periodic system criticality analysis, a disaster recovery plan, an emergency mode operation plan, and procedures for testing and revision of such plans."*

## A note about the layout of this book

*HIPAA Security Made Simple for Physician Practices* mirrors the structure of the HIPAA security rule. Each chapter is divided into sections, and each section is identified by the standard or implementation specification that is the subject of that section. The actual standard or implementation specification language is highlighted in bold at the start of each section. The tab on the edge of each page identifies the standard or implementation specification associated with that page.

Standard or Implementation  
Specification title




### Security Awareness and Training

---

***§ 164.308(a)(5) Required standard***

*“A covered entity must, in accordance with § 164.306, implement a security awareness and training program for all members of its workforce (including management).”*



Standard or Implementation  
Specification text

# HCPro

## Order your copy today!

Please fill in the title, price, order code and quantity, and add applicable shipping and tax. For price and order code, please visit [www.hcmarketplace.com](http://www.hcmarketplace.com). If you received a special offer or discount source code, please enter it below.

Title	Price	Order Code	Quantity	Total
				\$
<b>Your order is fully covered by a 30-day, money-back guarantee.</b>			<b>Shipping*</b> (see information below)	\$
			<b>Sales Tax**</b> (see information below)	\$
			<b>Grand Total</b>	\$

**Enter your special Source Code here:**

Name

Title

Organization

Street Address

City

State

ZIP

Telephone

Fax

E-mail Address

**\*Shipping Information**

Please include applicable shipping. For books under \$100, add \$10. For books over \$100, add \$18. For shipping to AK, HI, or PR, add \$21.95.

**\*\*Tax Information**

Please include applicable sales tax. States that tax products and shipping and handling: CA, CO, CT, FL, GA, IL, IN, KY, LA, MA, MD, ME, MI, MN, MO, NC, NJ, NM, NY, OH, OK, PA, RI, SC, TN, TX, VA, VT, WA, WI, WV.

State that taxes products only: AZ.

**BILLING OPTIONS:**

Bill me  Check enclosed (payable to HCPro, Inc.)  Bill my facility with PO # \_\_\_\_\_

Bill my (✓ one):  VISA  MasterCard  AmEx  Discover

Signature

Account No.

Exp. Date

(Required for authorization)

(Your credit card bill will reflect a charge from HCPro, Inc.)

**Order online at [www.hcmarketplace.com](http://www.hcmarketplace.com)**

**Or if you prefer:**

**MAIL THE COMPLETED ORDER FORM TO:** HCPro, Inc. P.O. Box 1168, Marblehead, MA 01945

**CALL OUR CUSTOMER SERVICE DEPARTMENT AT:** 800/650-6787

**FAX THE COMPLETED ORDER FORM TO:** 800/639-8511

**E-MAIL:** [customerservice@hcpro.com](mailto:customerservice@hcpro.com)

© 2008 HCPro, Inc. HCPro, Inc. is not affiliated in any way with The Joint Commission, which owns the JCAHO and Joint Commission trademarks. Code: EBKPDF

P.O. Box 1168 | Marblehead, MA 01945 | 800/650-6787 | [www.hcmarketplace.com](http://www.hcmarketplace.com)