# Content

About the Author ................................................................. vi

Acknowledgments .............................................................. vii

Preface .................................................................................. viii

Introduction .............................................................................. 1

Terms .................................................................................... 1

All About Policies ............................................................... 3

What Are HIPAA Policies? ................................................... 7

How to Use This Book ......................................................... 8

Section I: Where Privacy and Security Intersect .................. 11

A. Roles and Responsibilities .............................................. 13

B. Combined Privacy and Security Policies ......................... 27

Section II: Privacy ............................................................... 47

Other Regulations ............................................................... 47

Forms ................................................................................... 48

A. Covered Entity Use and Disclosure of PHI ....................... 48

B. Individual Privacy Rights Concerning PHI ......................... 85

Section III: Security ............................................................ 121

A. Administrative Safeguards .............................................. 122

B. Physical Safeguards ......................................................... 139

C. Technical Safeguards ....................................................... 154

Appendix ............................................................................... 171

Glossary of HIPAA Terms .................................................... 171

---

The No-Hassle Guide to HIPAA Policies
Policies and Forms

Section I
Policy 1: Designation of Privacy Officer .............................................................. 15
Form 1: Chief Privacy Officer Job Description ...................................................... 16
Form 2: Chief Information Security Officer Job Description .............................. 17
Policy 2: Information Security Program Governance ........................................ 19
Policy 3: Information Asset Protection Responsibility ........................................ 22
Policy 4: Sanctions for Privacy and Security Violations ...................................... 29
Policy 5: Confidential Data Protections ............................................................... 32
Policy 6: Privacy and Security Incident Response and Breach Notification .......... 34
Policy 7: Minimum Necessary Access and Disclosure ......................................... 37
Policy 8: Document Retention ........................................................................... 38
Form 3: Confidentiality Acknowledgment .......................................................... 39
Policy 9: Managing Business Associates ............................................................ 40

Section II
Policy 10: Uses and Disclosures of PHI for Treatment, Payment, and Healthcare Operations ....................................................... 51
Policy 11: Uses and Disclosures of PHI Not Requiring Permission or Opportunity to Agree or Object ........................................ 53
Policy 12: Uses and Disclosures of PHI for Research ......................................... 58
Form 4: Request for Waiver of Authorization for Research ................................ 65
Policy 13: Uses and Disclosures for PHI for Care Involvement and for Notification .............................................................................. 67
Policy 14: Uses and Disclosures of PHI in Facility Directories ............................ 69
Form 5: Directory Preferences ........................................................................... 71
Policy 15: Uses and Disclosures of PHI for Fundraising .................................... 72
Policy 16: Use and Disclosure of PHI in Limited Data Sets ................................. 74
Policy 17: Use and Disclosure of De-identified Information ................................ 76
Policy 18: Uses and Disclosures of PHI Requiring Authorization ........................ 78
Form 6: Authorization for Use or Release of Your Health Information ................. 82
Policy 19: Privacy Notice Content and Delivery ................................................. 87
Form 7: Privacy Notice—Acknowledgment of Receipt ....................................... 90
Policy 20: Right to Inspect, Copy, and Request Transmittal of One’s PHI .............. 96
Form 9: Request to Review, Obtain a Copy, or Send a Copy of My Health Records ................................................................. 99
Form 10: Denial (and Review of Denial) of Patient Access to Health Records ........ 101
Form 11: Denial of Request to Review or Obtain a Copy of Your Health Records ........................................................................ 103
Policy 21: Right to Request Amendment of One’s PHI ....................................... 104
Policy 22: Right to Request Restrictions on One’s PHI ....................................... 108
Policy 23: Right to Accounting of Disclosures of One’s PHI ............................... 112
Policy 24: Right to Receive Confidential Communications ................................ 117
Form 12: Request for Amendment of Your Health Information .......................... 106
Form 13: Request for Restriction on Use or Disclosure of Health Information ..... 110
Form 14: Request for Accounting of Disclosures of My Health Information ........ 116
Form 15: Request for Confidential Communications .......................................... 119
### Section III

<table>
<thead>
<tr>
<th>Policy</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy 25</td>
<td>Information Security Management Program</td>
<td>125</td>
</tr>
<tr>
<td>Policy 26</td>
<td>Information Security Classification</td>
<td>127</td>
</tr>
<tr>
<td>Policy 27</td>
<td>Information System Activity Review</td>
<td>130</td>
</tr>
<tr>
<td>Policy 28</td>
<td>Supervision of Unauthorized Individuals</td>
<td>132</td>
</tr>
<tr>
<td>Form 16</td>
<td>Access Termination Checklist</td>
<td>133</td>
</tr>
<tr>
<td>Form 17</td>
<td>Authorizer Form</td>
<td>134</td>
</tr>
<tr>
<td>Form 18</td>
<td>Request for Access to the EMR System</td>
<td>135</td>
</tr>
<tr>
<td>Policy 29</td>
<td>Computer Security Contingency Plan</td>
<td>137</td>
</tr>
<tr>
<td>Policy 30</td>
<td>Regulatory Compliance Auditing of Computer Security</td>
<td>138</td>
</tr>
<tr>
<td>Policy 31</td>
<td>Facility Security</td>
<td>141</td>
</tr>
<tr>
<td>Policy 32</td>
<td>Walk-Around Security Reviews</td>
<td>143</td>
</tr>
<tr>
<td>Form 19</td>
<td>Walk-Around Security Audit</td>
<td>144</td>
</tr>
<tr>
<td>Policy 33</td>
<td>Review of Security-Related Facilities Work</td>
<td>146</td>
</tr>
<tr>
<td>Policy 34</td>
<td>Acceptable Computer Use</td>
<td>147</td>
</tr>
<tr>
<td>Policy 35</td>
<td>Security of Portable Computers and Media</td>
<td>149</td>
</tr>
<tr>
<td>Policy 36</td>
<td>Off-Site Work Security</td>
<td>151</td>
</tr>
<tr>
<td>Form 20</td>
<td>Working Off-Site Security Agreement</td>
<td>153</td>
</tr>
<tr>
<td>Form 21</td>
<td>Integrity of PHI at ABC Organization</td>
<td>156</td>
</tr>
<tr>
<td>Policy 37</td>
<td>Encryption of Confidential Data Over the Internet and Wireless Networks</td>
<td>158</td>
</tr>
<tr>
<td>Policy 38</td>
<td>Disposal of Confidential Information</td>
<td>159</td>
</tr>
<tr>
<td>Policy 39</td>
<td>Electronic Mail Use</td>
<td>162</td>
</tr>
<tr>
<td>Policy 40</td>
<td>Firewall Management</td>
<td>166</td>
</tr>
</tbody>
</table>

Download the sample policies and forms in this book with the purchase of this product.
About the Author

Kate Borten, CISSP, CISM

Kate Borten, president and founder of The Marblehead Group, brings to clients her unique combination of expertise in information security, privacy, and IT from more than 20 years in the healthcare industry. She led the corporatwide security program at Massachusetts General Hospital in Boston and, as chief information security officer, she established the first enterprisewide information security program at CareGroup and Beth Israel Deaconess Medical Center, a major healthcare system based in Boston.

Borten is a nationally recognized expert on HIPAA and health information privacy and security and a frequent speaker on these topics. She is the author of The HIPAA Omnibus Rule: A Compliance Guide for Covered Entities and Business Associates, The HIPAA Omnibus Rule Toolkit: A Covered Entity and Business Associate Guide to Privacy and Security, HIPAA Security Made Simple: Practical Compliance Advice for Covered Entities and Business Associates, and H-Mail: HIPAA and HITECH Privacy and Security Training Reminders for Healthcare Staff, all published by HCPro, a division of BLR. She is also the author of 11 specialized HIPAA training handbooks for behavioral health staff; business associates; coders, billers, and health information management staff; executive, administrative, and corporate staff; healthcare staff; home health staff; long-term care staff; nursing and clinical staff; nutrition, environmental services, and volunteer staff; physicians; and registration and front office staff, also published by HCPro. She is a contributing author to Auerbach Publications' Information Security Management Handbook and a contributor to HIPAA privacy and security newsletters.

The Marblehead Group (marbleheadgroup.com) provides HIPAA privacy and security program development and regulatory compliance, training, risk assessment, and HIPAA compliance auditing to the healthcare industry. Borten's clients include the full spectrum of public and private sector healthcare providers, health plans, and their business associates.
Acknowledgments

HCPRO and the author gratefully acknowledge the following individuals and organizations for generously contributing source material to this book to complement that created by the author in her work as a HIPAA consultant.

Chris Apgar, CISSP
President
Apgar & Associates, LLC
Portland, Ore.

Holly Ballam, RHIA, RN
Data Abstractor/Clinical Nurse
Performance Assessment and Regulatory Compliance
Beth Israel Deaconess Medical Center
Boston, Mass.

John R. Christiansen, JD
Attorney
Christiansen IT Law
Seattle, Wash.

Rick Ensenbach, CISSP-ISSMP, CISA, CISM, CCSFP
Manager of Risk Advisory & Forensic Services
WIPFLi
Eau Claire, Wis.

Kelley L. Meeusen, RHIT, CSS
HIM Distance Learning Instructor
Tacoma Community College
Tacoma, Wash.

Partners Healthcare System, Inc.
Boston, Mass.

Peggy Presbyla, RHIA, CHP
Operations Manager
Upstate University Hospital at Community General
Syracuse, N.Y.
Preface

The U.S. Department of Health and Human Services (HHS) published the HIPAA Omnibus Rule affecting all HIPAA-defined covered entities (CE) and their business associates (BA) January 25, 2013. The Omnibus Rule is formally known as *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule*.

Enforced beginning in September 2013, this sweeping set of regulations expands patient privacy rights and organizations’ obligations. It implements portions of the 2009 American Recovery and Reinvestment Act (Recovery Act), also known as the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Genetic Information Nondiscrimination Act (GINA), expands the definition of BA, and strengthens the HIPAA Breach Notification Rule.

Revisions in this edition that pertain to the Omnibus Rule apply to the following privacy rights and organizational responsibilities:

- **Privacy and security incident response.** Responding to a privacy or security incident includes determining what, if any, breach notification is required by law and/or organizational policy. The Omnibus Rule’s enhanced breach determination and notification process must be incorporated into policies and procedures.

- **BA contracts.** The Omnibus Rule clarifies and expands the definition of a BA. Further, the Omnibus Rule requires explicit language to ensure that the full chain of BAs understand they now are directly subject to, and agree to adhere to, the entire HIPAA Security Rule and portions of HIPAA’s Privacy and Breach Notification Rules.

- **Uses and disclosures of protected health information (PHI) for fundraising.** The Omnibus Rule permits healthcare providers to use more types of PHI for fundraising purposes, but also requires these CEs to follow easier opt-out methods.

- **Uses and disclosures of PHI for marketing and sale.** The Omnibus Rule clarifies what constitutes marketing, and it reinforces the prohibition against marketing with PHI and sale of PHI without a HIPAA-compliant authorization.

- **Right to inspect, copy, and request transmittal of one’s PHI.** The Omnibus Rule requires organizations that maintain PHI electronically to comply when patients request their PHI in electronic form. Further, organizations also must comply when patients request PHI transmittal to designated third parties.
• **Right to request restrictions on one's PHI.** Previously, patients had the right to request certain restrictions on how their PHI was used and disclosed under the Privacy Rule, but CEs were not required to agree. Now, there is one instance in which CEs generally must agree. Patients may request that providers not disclose to a health plan PHI related to a specific service or item when it has been paid for in full out-of-pocket. In this instance, the request must be honored for disclosures that would have been made for payment or healthcare operations (i.e., not treatment).

**Notice of privacy practices.** CEs are required to add language to their privacy notices to reflect new Omnibus Rule restrictions and rights, including the duty of CEs to notify patients and plan members of a breach of their PHI. Revised notices should be handed to all new patients (or mailed to new plan members). Revised privacy notices must be posted on CEs’ websites and displayed prominently in public areas such as waiting rooms.

In conclusion, the Omnibus Rule also includes the final Enforcement Rule specifying civil monetary penalties for failure to comply with HIPAA rules. Congress increased these in the HITECH Act, and HHS has implemented them. The tiered civil penalties are now final as described in the following chart:

<table>
<thead>
<tr>
<th>TIER</th>
<th>PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person did not know (and by exercising reasonable diligence would not have known) that a provision was violated</td>
<td>$100–$50,000 for each violation Up to $1,500,000 for all such violations of an identical provision in a calendar year</td>
</tr>
<tr>
<td>Violation due to reasonable cause and not to willful neglect</td>
<td>$1,000–$50,000 for each violation Up to $1,500,000 for all such violations of an identical provision in a calendar year</td>
</tr>
<tr>
<td>Violation due to willful neglect but corrected within 30 days of knowing, or date when entity exercising due diligence would have known, of the violation</td>
<td>$10,000–$50,000 for each violation Up to $1,500,000 for all such violations of an identical provision in a calendar year</td>
</tr>
<tr>
<td>Violation due to willful neglect and not corrected within 30 days of knowing, or date when entity exercising due diligence would have known, of the violation</td>
<td>$50,000 for each violation $1,500,000 for all such violations of an identical provision in a calendar year</td>
</tr>
</tbody>
</table>

Note that there is no overall cap on the amount of civil penalties. An investigation by HHS revealing a CE's or BA's failure to comply with numerous regulatory requirements could result in fines totaling many millions of dollars.
Introduction

Policies are essential for all but the smallest organizations to operate smoothly. Clearly written policies and their associated procedures describe the rules by which the workforce operates. They help ensure consistency in how work processes are performed, and they establish expectations for employee conduct.

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) directed the U.S. Department of Health and Human Services to write privacy and security regulations. The Privacy and Security Rules were finalized in late 2000 and in 2003, respectively. The rule writers understood the importance of written policies and, thus, required covered entities (CE) subject to these rules to formulate and abide by a multitude of policies.

But creating policies—and it can be a creative process—is not always simple. The purpose of this book is twofold: It provides a variety of policies and other documents to ease the effort, and it helps the reader understand what constitutes a good policy that is meaningful and enforceable.

Terms

Before tackling the job of writing or revising policies, it's helpful to have a clear understanding of several related but different terms.

Policy: A policy is usually a high-level statement reflecting a principle or commitment made by the highest level of management. Policies should stand the test of time; and although they should be reviewed periodically, they should not require frequent changes. It is necessary to review and approve new and amended policies through a documented process that validates them. Organizationwide policies should be approved by a CEO or similar high-level officer. Policies should not contain procedural details that may vary in different parts of the organization or require frequent changes. Nor should they specify technical details that may not be universal and may change without affecting the policy intent.
Introduction

*Example:* HIPAA’s Privacy Rule gives patients certain rights, such as the right to access one’s own records (with certain limited exceptions). This right must be affirmed in a policy at every CE. It is a right that is likely to continue to exist, and it is a right that applies throughout a healthcare organization.

Sometimes a policy will contain general rules that give it more detail and apply consistently throughout the organization. These are not the same as detailed procedures.

**Procedure:** Procedures are the detailed, step-by-step instructions for how the workforce is to accomplish a task while complying with policies. Typically, policies and procedures do not have a one-to-one correlation. One policy can generate multiple procedures, and one procedure often supports multiple policies.

Procedures usually are written by or with input from individuals who perform the tasks. When necessary, changing a procedure is usually a simple process, with minimal review, handled by the individuals using the procedure.

*Example:* HIPAA’s Security Rule requires a controlled process for establishing user access to a computer system containing electronic protected health information (ePHI). There should be procedures, or step-by-step instructions, for creating user accounts in each system. A policy should require that anyone granted access to such a system have a unique user ID. To support and enforce that policy, the procedures should prohibit the creation of generic user IDs. (Some organizations may permit an unusual exception if it has been appropriately authorized. The exception process also should be documented in this instance.)

*Example:* HIPAA requires CEs to distribute copies of their privacy notices to new patients. This requirement should be stated in a global policy. In a healthcare facility that treats both ambulatory and admitted patients, the detailed procedures for delivery of the privacy notice are likely to differ in the ambulatory registration process and the inpatient admissions process.

**Standard operating procedure (SOP):** HIPAA rules permit small organizations to use SOPs instead of creating separate policies and procedures. The SOP combines one or more policy statements with a working procedure. This is appropriate in a small office setting where everyone follows the same procedures and there is less need for layers of documentation.
Standard: The term standard is often used in a technology context. Technical details should be separate from policies because:
   a. They are not directly relevant to the policy
   b. A senior executive approving a policy is not likely to be able to evaluate the standard
   c. Some technical standards should be treated as confidential
   d. Technical standards may change independent of the policy

Example: A policy may require that user authentication meet organization standards before access to the organization's electronic resources is allowed. An organization specifies its current technical standards for authentication separately. There may be password standards, including minimum length, complexity, and frequency of change. There also may be standards for other types of authentication, such as tokens and biometrics. The technical experts should be entrusted with setting and maintaining technical standards. Changes to those standards, such as requiring longer passwords, would not require changes to the policy.

Guideline: The term guideline is best understood in comparison to policies and procedures. Policies must be followed or workforce members may be sanctioned. There is an expectation that standards will be followed unless there are exceptions—usually for technical reasons such as legacy computer systems with limited flexibility. Procedures should be followed, or if they are ineffective, they should be changed. However, a guideline is simply a suggestion, and it usually is unenforceable. When workforce adherence to established rules is expected, organizations should avoid using guidelines except, perhaps, as a complement to policies, procedures, and standards.

All About Policies

Content
An effective policy must be very clear and unambiguous. A reader should be able to easily understand the intent of the policy, its scope and application, and potential consequences for failure to adhere to its requirements. An effective policy should include the following information.

Heading: Include a title that identifies the policy in a meaningful and unambiguous manner. In all but the smallest organizations, it is helpful to assign a unique identifier, such as “IS 123” for Information Security policy number 123. Even small organizations store important documents in electronic files, and a standard numbering system is important for categorizing and retrieving policies and related documents.
Introduction

The heading section also should include the name and title of the policy’s sponsor so that questions are directed to the appropriate person. Typically, as the subject matter experts, privacy officers sponsor privacy policies and information security officers sponsor information security policies.

**Policy statement:** This section is usually brief and to the point. Avoid trying to cover too many subjects in a single policy statement. Otherwise, the result could be an overly complicated policy. Test the policy statement by reading it alone to ensure that it states a commitment or principle to be followed.

*Example:* “All electronic data classified as Confidential or higher must be encrypted when transmitted over public networks and wireless networks.”

**Purpose:** This should explain the fundamental reason for having a specific policy. Members of the workforce are more likely to remember and follow a policy if they understand its purpose and value.

*Example:* “The purpose of this policy is to protect individual privacy and data confidentiality by preventing unauthorized entities from reading the data while in transit over networks beyond our control.”

**Scope:** This equally important section should describe to whom the policy does and does not apply. It also should explain other circumstances or classes of data that are either in scope or out of scope.

*Example:* “This policy applies to all data under this organization’s control that are classified as Confidential or Highly Confidential. Encryption of data in a lower classification level is discretionary. This policy applies to our business associates and other business partners if and when they transmit Confidential or Highly Confidential data on our behalf.”

**General rules:** This section is not included in every policy, but there are times when it is helpful to state general rules, such as mandatory underlying conditions. Note that general rules are not procedures, but they are likely to be incorporated in them.

Many HIPAA privacy policies include general rules that are explicit regulatory requirements, such as those related to the privacy notice.
Introduction

Example: “The following statement must be displayed at the top of the notice:

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”

Regulations: Some organizations cite specific regulations in their policies. HIPAA Privacy Rule–related policies often directly reflect a specific standard in the rule. In other instances, a policy might incorporate multiple regulations, in part or in whole. Sometimes a policy simply reflects good practices that only indirectly demonstrate regulatory compliance.

References: Standard terms, whether defined by the organization or by regulation, should be explained separately in a common glossary. This helps ensure that definitions are included in a single official source. In electronic documents, terms can be links to the organization’s official glossary of terms.

Example: “See Glossary for definition of Confidential Data, Business Associate, and PHI.”

Related documents: This section may include links to related policies, procedures, forms, standards, and other formal documents in the organization’s libraries.

Example: “Information Classification Policy, Encryption Standards”

Monitoring and enforcement: A policy has limited value if there is no assigned responsibility for monitoring or no plan for monitoring compliance. Furthermore, failure to monitor or enforce a policy may result in legal liability for the organization.

Example: “This encryption policy will be monitored and enforced by the Information Security Department.”

In this example, the information technology (IT) and security teams have collaborated to monitor outbound email messages to help ensure that encryption is being used when required by the policy.

Approval: Include the name of the executive or high-level committee that approved the policy and any subsequent revisions.
Introduction

Example: “Approved by the General Executive Committee April 1, 2004. Revision approved April 1, 2005.”

Review: Specify the review cycle (e.g., annually), the most recent review date, and perhaps the person or team that reviewed the policy. Like the monitoring and enforcement section, the review information’s inclusion in the policy demonstrates a commitment to assigning responsibility and conducting periodic reviews.

Example: “Annual review cycle. Last reviewed April 2007.”

Revision history: List revision dates, note the changes, and state by whose authority or approval the changes were made. This information is required because policies related to HIPAA Privacy and Security Rule compliance are subject to the six-year document retention requirement. Organizations must know the effective date range and version of each HIPAA-relevant policy. For example, if a breach or legal issue related to a workforce member’s behavior several years ago arose, the affected organization might be required to produce versions of relevant policies as they existed at that time.

Example: “Policy statement extended to include ‘and wireless networks’ April 1, 2005, as authorized by the ISO.”

Tips

Writing effective policies isn’t simple. Avoid the following pitfalls:

Policies that contain too much detail. Generally, the larger the organization, the less detail should appear in its policies. Unless the organization is very small, include the how-to details in separate procedures and standards. Otherwise, the details may need to be changed often, or they may not apply universally. Conversely, general rules sometimes do have a place in policies. For example, a policy describing when PHI can be released with authorization may include details from the HIPAA Privacy Rule. These supplement the policy statement and are not how-to procedures.

Policies without exceptions. Occasionally there are legitimate reasons for an exception to a policy. Without inviting exceptions, organizations should be proactive and prepared. A standard exception process permits adequate review, oversight, consistency, and follow-up. Organizations can create a procedure and form to capture the requestor’s identity, the exception, and the rationale for it.
Policies that are unrealistic. Don’t write a policy that cannot be followed. For example, a health-care organization that routinely uses email to communicate with other facilities about its patients might write a policy requiring email encryption. But if the organization does not implement an encryption solution, email will continue to be sent via the Internet in knowing violation of the policy. This creates a legal vulnerability and it suggests to the workforce that management doesn’t really expect policies to be followed.

Policies that can’t be monitored. While writing a policy, consider how to monitor the environment and workforce for compliance. This can present a challenge. For example, HIPAA requires organizations to protect PHI even when it’s used or accessed outside the facility, such as at an employee’s home. Organizations can write a policy requiring certain off-site controls, but they also should consider developing a process to monitor off-site activity. Some organizations do this by reserving the right to perform in-home inspections of teleworkers to ensure compliance and limit risk.

What Are HIPAA Policies?

In many healthcare organizations, the impetus for writing privacy and security policies is compliance with HIPAA. Hence, the healthcare industry often refers to “HIPAA policies” as shorthand for those policies required by HIPAA. In fact, while some policies specifically address a unique HIPAA requirement, such as the requirement to provide patients and plan members with copies of the organization’s privacy notice, many policies required by these regulations are simply good practice, especially those related to security.

That raises the question of the scope of so-called HIPAA security policies. Security professionals generally agree that an organization cannot adequately protect a subset of data, such as PHI, unless security protections extend to the full environment, including connected networks and physical facilities. For example, if a tightly controlled ePHI server and a more loosely controlled test server occupy the same network segment, unauthorized access to ePHI could occur from the test server by watching network traffic.

Therefore, although beyond the scope of HIPAA’s Security Rule, this book presents security and certain other policies in broader terms to safeguard all protected information assets, including PHI.

An additional policy scope consideration is security of nonelectronic forms of PHI. Although HIPAA’s Security Rule focuses on electronic PHI, HIPAA’s Privacy Rule requires administrative, physical, and
Introduction

technical security protections for all forms of PHI, whether oral, paper, or other media. Thus, organizations must include security of nonelectronic PHI in their policies and procedures for regulatory compliance. It’s also simply good business practice.

When policies are written broadly to address all of an organization’s important information assets, rather than narrowly with “HIPAA” in the title, there are several ways for an organization to demonstrate HIPAA compliance. The scope section of each such policy can use language such as “This policy applies to all information assets classified as Confidential or higher, including Protected Health Information.” In addition, organizations can develop and maintain a spreadsheet mapping the HIPAA Privacy and Security Rule standards and specifications to supporting documents.

How to Use This Book

HIPAA requires healthcare organizations to establish permanent privacy and security programs. Privacy and security are not simply projects to be completed. A work culture that is attuned to privacy rights and security safeguards is the result of diligence and continuous program improvement. This includes routine, periodic review to identify gaps and out-of-date policies.

This book is helpful whether your organization is developing privacy and security policies for the first time, filling in gaps, or seeking improvement to take your programs to the next level of maturity.

While this book will make privacy and security document development easier, no book of this type can be used in its entirety without some customization to fit your organization’s particular needs, legal requirements, and culture.

The Privacy and Security Rule standards and specifications are sometimes very explicit and directive. This enables organizations to understand exactly what they should do to comply with HIPAA. Examples include:

• Instructions regarding delivery of the privacy notice
• Instructions for authorization form content
• Requirement that everyone who accesses ePHI have a unique user ID
However, the rules are also frustratingly vague in other areas. This is largely because the rules had to be written as “one size fits all,” and the range of organizations subject to the rules is vast, from multistate health plans covering millions of individuals to single-practitioner offices. Because the circumstances, capabilities, and risks differ in each setting, some standards and specifications are expressed as high-level principles without explicit instructions that explain how to achieve the principle.

The requirement for integrity and data authentication is a good example, because integrity, along with confidentiality and availability, is one of the three core components of information security.

To meet these sorts of standards, organizations are expected to understand what is intended and to determine the appropriate measures for their particular circumstances. More latitude is permitted with respect to how an organization responds to these standards. The solutions, which can include a combination of policies, procedures, and technologies, will vary from one organization to another.

Therefore, some documents in this book are directive, and an organization’s only choice is presentation style. However, other documents should be customized, using the online Appendix on the companion website (www.hcpro.com/downloads/11884), based on each organization’s factors, such as size, complexity, resources, risk level, and risk posture.

Some policies presented in this book may be combined with others or separated into several documents. This is usually a matter of style. The sample policies and forms contained in this book provide an array of stylistic choices with respect to detail, language, organization, acronym use, and appearance, designed to help organizations write policies that accurately reflect both their corporate culture and their ongoing commitment to patient privacy and information security.

For simplicity, the policy examples in this book include the following sections:

- Title (but not the full heading, including sponsor, etc.)
- Policy statement
- Purpose
- Scope
- General rules (when applicable)
Introduction

However, they will not include the following sections because their repetitive or organization-specific nature does not contribute to the usefulness of the sample policies:

- References
- Related documents
- Monitoring and enforcement
- Approval
- Review cycle and dates
- Revision history

Final reminders

First, these documents must be customized to reflect the circumstances of each individual organization.

Second, these documents do not constitute a complete, final set of privacy and security policies. New and revised policies need to be added periodically to an organization's policy set to reflect the dynamic nature of privacy and security risks and regulatory requirements.

Finally, while adoption of these and other policies is an important step toward managing risk, it does not eliminate risk of a breach, nor does it guarantee regulatory compliance.

A glossary including selected terms with specific meaning in the context of HIPAA is included at the end of this book and in the online Appendix. The source of definitions provided is Title 45 of the Code of Federal Regulations (CFR) Parts 160 and 164. The glossary also includes instructions for accessing the most current regulations and definitions online.

Editor's note: Access the online Appendix at www.hcpro.com/downloads/11884.
This section contains documents directly relevant to both privacy and information security.

Everyone is familiar with the words privacy and security, but what do these terms mean to the experts and what is the relationship between privacy and security?

**Information privacy** refers to controlling your personal information so that you have reasonable expectations as to how it will be used and released to others. Information privacy requires that governments and organizations respect key principles:

- **Boundaries**: Limits on the collection and use of your personal information; information collected for a stated purpose may not be used for a different purpose
- **Security**: The obligation to protect and preserve the confidentiality, integrity, and availability of your information
- **Consumer control**: The right to inspect the information about you, obtain a copy, have corrections made, and know to whom the information has been released
- **Accountability**: Penalties for failure to implement and enforce these principles
- **Public responsibility**: To determine the appropriate balance between individual privacy and the public good

**Information security** is commonly defined as the assurance of confidentiality, integrity, and availability of the protected information.

- **Confidentiality**: Only those individuals (and computer processes) that have been authorized can access the information
- **Integrity**: The information can be relied upon and has not been inappropriately altered or destroyed
- **Availability**: When needed, the information is available to those authorized to access it
These descriptions of privacy and security illustrate that we cannot have privacy unless we also have security. They are different, but privacy depends on security, particularly the assurance of confidentiality.

This explains why Congress called for both privacy and security in enacting HIPAA in 1996, yet also expected separate sets of regulations for these two topics. Notably, different teams of experts wrote the two rules.

Inclusion of the so-called “Mini–Security Rule” within the Privacy Rule is further indication that privacy depends on security. Although few specifics are provided, the Privacy Rule requires administrative, physical, and technical security safeguards to shield protected health information (PHI) in all forms. The Security Rule adds details and describes the security safeguards that must be implemented for electronic PHI (ePHI).

When the proposed Privacy Rule was announced, the secretary of the U.S. Department of Health and Human Services (HHS) reserved the right to delay its enforcement if the Security Rule had not yet been implemented, thereby reinforcing the fact that there cannot be privacy without security.

To meet the goals of privacy and security, HIPAA covered entities (CE) must establish formal privacy and security programs with assigned roles and responsibilities that reflect those professions. The programs must be closely aligned, but those responsible for the programs should recognize how they complement as well as differ from each other. This section includes job descriptions and related documents describing roles.

Conversely, it is less important that the general workforce understand the difference between privacy and security. This section includes several documents, such as a sanctions policy, required by both the Privacy Rule and the Security Rule, that are likely to be more effective when they address both privacy and security.

Often, a privacy incident or breach is also a security incident or breach, and the converse is also true. The workforce should be able to recognize a potential problem and report it internally, without having to label it as either privacy or security. In case of an incident or breach, privacy and security officers should work together to sort out what happened and determine how privacy and security are affected.
Finally, this section combines some documents for ease of administration and HIPAA compliance because both rules require many of the same administrative processes such as document retention.

A. Roles and Responsibilities

There are various ways in which organizations formally establish the privacy officer (PO) and information security officer (ISO) roles, as required by HIPAA. Generally, the larger and more risk-averse an organization, the more likely these roles will be full-time positions with staff. Also, organizations having separate facilities or divisions commonly will have an enterprisewide “chief” PO and ISO, with local POs and ISOs at each division.

Whether a CE is large, medium size, or even small, official recognition of these roles and their responsibilities is required by HIPAA. Therefore, organizations are wise to create job descriptions and commit to these roles in policy.

About the policies and forms in this section

Policy 1: Designation of Privacy Officer
This sample policy establishes the role and primary responsibilities of the PO. It includes some information about the role's responsibilities. It is advisable to also develop a PO job description that more fully describes responsibilities, qualifications, reporting structure, and other relevant information.

The “Designation of Privacy Officer” policy alternatively could be written for a PO role with broad responsibility for protecting the privacy of patients and also employees, chief professional staff, and any others with a privacy stake.

Form 1: Chief Privacy Officer Job Description
This form is a sample (partial) job description for the (chief) PO.

Form 2: Information Security Officer Job Description
This form is a sample (partial) job description for the (chief) ISO.

Policy 2: Information Security Program Governance
This sample policy describes many roles in information security program governance. The PO and ISO are the most visible players, but they can’t achieve success without the active involvement of others.
• Organizations should establish a committee to provide further oversight, guidance, and support to the PO and ISO

• Managers have day-to-day responsibility for overseeing staff and other duties such as initiating access change and termination requests

• Every individual in the workforce is responsible for his or her own behavior and for reporting suspected privacy and security violations

**Policy 3: Information Asset Protection Responsibility**

This policy is similar in concept to sample Policy 2 but includes some variations.
**Policy 1** Designation of Privacy Officer

**Title:** Designation of Privacy Officer

**Policy:** This organization is committed to ensuring the privacy of patient health information (protected health information [PHI] as defined by HIPAA). Therefore, we will create and maintain the role of Privacy Officer (PO) to plan and oversee our privacy program.

**Purpose:** Not only is this role required by HIPAA’s Privacy Rule, but it is important to the success of our privacy program. The PO will be a single point of authority and responsibility regarding patient privacy matters.

**Scope:** This organizationwide role is responsible for ensuring that our privacy program protects PHI in all forms.

**GENERAL RULES:**

1. The PO is responsible for overseeing all policies and procedures regarding:
   a. How we use and disclose PHI
      - When no permission is required
      - When an opportunity to agree or object is required
      - When an authorization is required
   b. Our privacy notice
      - Content
      - Delivery
      - Posting
   c. Support of our patients’ privacy rights as defined by HIPAA’s Privacy Rule and other state and federal laws and regulations, including, but not limited to:
      - The right to inspect and copy
      - The right to request amendment
      - The right to confidential communications
      - The right to request restrictions on uses/disclosures
   d. How we handle privacy questions and complaints

2. The PO, with the Information Security Officer (ISO), is responsible for:
   a. Privacy and security incident response processes
   b. Privacy/security violations sanctions policy and guidelines
   c. Managing Business Associate privacy and security compliance
   d. Oversight of workforce privacy and security training
This updated toolkit from one of the most highly respected HIPAA experts in the healthcare industry remains the essential guide for developing HIPAA privacy and security policies. Kate Borten, a prolific author and sought-after national speaker on HIPAA compliance, has developed numerous policies, procedures, and forms as a chief information security officer and consultant.

Covered entities and their business associates (BA) can customize the 40 sample policies and 21 sample forms in this toolkit to meet the needs of their organizations and satisfy longstanding HIPAA requirements and new Omnibus Rule requirements. The sample policies and forms from Borten and leading healthcare organizations are also available in the online Appendix.

Revisions in this edition facilitate compliance with new Omnibus Rule requirements that apply to the following privacy rights and organizational responsibilities:

- Privacy and security incident response
- BA contracts
- Uses and disclosures of protected health information (PHI) for fundraising
- Uses and disclosures of PHI for marketing and sale
- Right to inspect, copy, and request transmittal of one’s PHI
- Right to request restrictions on one’s PHI
- Notice of privacy practices

Healthcare officers charged with compliance will find that The No-Hassle Guide to HIPAA Policies continues to be the blueprint for compliance excellence.