HIPAA in Clinical Trials

A Practical Guide for Research Compliance

Lawrence H. Muhlbaier, Ph.D.
## CONTENTS

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

Acronym Guide ................................................................. vii

Introduction ................................................................. viii

Chapter 1: Introduction to HIPAA ........................................ 1

  What is HIPAA? ................................................................. 4
  Who is covered by HIPAA? .................................................. 5
  HIPAA’s effect on research .................................................. 6
  Patient identifiers ............................................................... 7
  Deadlines ........................................................................... 7
  Definitions ........................................................................ 8

Chapter 2: Privacy Basics .................................................... 13

  Use and disclosure ............................................................... 15
  Permitted uses and disclosures ........................................... 18
  The minimum necessary rule .............................................. 21
  Implementation specifics ..................................................... 24
  The notice of privacy practices ........................................... 25
  HIPAA penalties ................................................................. 26

Chapter 3: Privacy Board v. IRB ........................................... 29

  What is a privacy board? ...................................................... 31
## Contents

**Chapter 4: New Authorization Requirements** ................................................. 33

- Necessary information for authorization .................................................. 35

**Chapter 5: Research Without Written Authorization** ............................... 39

-Waivers and alterations to authorizations ................................................ 41
- Reviews preparatory to research ............................................................. 42
- Research on decedent PHI ................................................................. 43

**Chapter 6: Changes to the Pre-screening Process** ................................... 45

- Reviews preparatory to research ............................................................. 49
- Choosing individuals from your facility ............................................... 50

**Chapter 7: Transition provisions and research** ....................................... 51

**Chapter 8: De-identification and Limited Data Sets** .............................. 55

- How to de-identify information ............................................................. 57
- Safe harbor ............................................................................................ 58
- Link fields ............................................................................................. 59

**Chapter 9: Patient Rights** ................................................................. 61

- Right to request restrictions ................................................................. 63
- Right to request specific communication .............................................. 66
- Right to an accounting of disclosures ................................................... 66
- Case scenario ....................................................................................... 69
- Right to request an amendment to PHI ................................................ 70
- Right to access PHI ............................................................................ 72
- Certificates of Confidentiality .............................................................. 77

**Chapter 10: Business Associates** ......................................................... 79
Contents

Who are your business associates? ................................................................. 81
Central laboratories ...................................................................................... 82
Drafting an agreement .................................................................................. 84
Comparison of business associate contracts and data use agreements ............. 86

Chapter 11: Security Expectations ................................................................. 91

Potential changes .......................................................................................... 94
The security officer ......................................................................................... 95
Risks to your facility ....................................................................................... 96
Security implementation ............................................................................... 98
Policies and procedures ............................................................................. 100
Physical safeguards .................................................................................... 102
Technical security services ....................................................................... 102
Encryption .................................................................................................. 105

Chapter 12: Training Tips ............................................................................. 107

Start training now ......................................................................................... 109
Training Tactics .......................................................................................... 110
General tips .................................................................................................. 111

Chapter 13: Frequently Asked Questions .................................................. 113

Appendix: Forms and Guidance Documents ............................................... 123

Notice of privacy practices ........................................................................ 126
Safe harbor de-identification chart .............................................................. 138
Decision tree for use and disclosure ........................................................... 141
HIPAA complaint reporting form ............................................................... 143
Data use agreement .................................................................................... 145

Using the files on your HIPAA in Clinical Trials CD/ROM ......................... 147

Index ............................................................................................................ 149
CHAPTER 1

Introduction to HIPAA
Chapter 1

Introduction to HIPAA

In 1996, Congress passed a revolutionary law and told you to know it — or else. But you had seven years to get it straight, and what did you need to know about “insurance portability” anyway?

Congress gave itself four years to implement new rules under this bill, also called the Kassebaum-Kennedy Act, and established a safety net of having HHS apply the law if they couldn’t get to it in the allotted time. Finally, on December 28, 2000, HHS was forced to act and released a 1,500-page regulation to the public. That report—laced with legal language—and its aftermath have become a growth industry for lawyers. By now you’ve found that the document is much more than its title suggests. It wends its way through and infiltrates every avenue and area of health care and research, from the candy stripers to the top of the administration and Boards of Directors. The document went from an afterthought to a bombshell.

Welcome to HIPAA.

The Health Insurance Portability and Accountability Act of 1996 brings sweeping changes, and the teeth to enforce these changes, at a time when medicine and research are already in flux. New technologies and innovative ideas are bringing change to health care daily, and you want to be part of the new era. Why can’t someone else be responsible for dealing with these new wide-ranging regulations? The simple answer is: It has to be you who is responsible, because you are on the front lines of research and health care.

HIPAA is set to change the lives of everyone involved in health care, and everyone is responsible for knowing how it will affect them. No institution can afford to drop the ball on this one. The underlying theme of the regulation for everyone linked to medicine and research is the protection of participant and
patient information based on HHS guidance. The rules are clearly spelled out, but implementing them could be difficult, as there is no precedent for much of what the regulations have set out to accomplish.

HIPAA is generally viewed in two ways. For some, it is a daunting, mammoth regulation that will provide mounds of extra work and increased confusion for an institution. For others, it is an effort to streamline practices across the board and accomplish the goals every researcher and health care worker already has: keeping patients safe and their privacy protected. But this regulation extends well beyond research data, prescriptions, and surgery. It gets to the heart of the patient’s value of safety and personal privacy that in the past may have been sacrificed for the sake of easier access to information or increased revenues.

What is HIPAA?

HIPAA covers three specific areas, including:

- **Insurance portability**
- **Fraud enforcement, or accountability**
- **Administrative simplification**

**Insurance portability** ensures that individuals moving from one health plan to another will have continuity of coverage and will not be denied coverage under “preexisting-conditions” clauses. Since most clinical trials do not bill directly to third-party insurance, this is not a crucial aspect of HIPAA for researchers.

**Accountability** significantly increases the federal government’s fraud enforcement authority in many different areas.

Although the first two are important to some institutions and employees, **administrative simplification** is the area that is most relevant to researchers and the area where most of the confusion surrounding the act resides. For anyone involved with clinical research, this is the most critical aspect of the act with which one should be familiar.

Administrative simplification received little attention when the law was first enacted, as its effective date was set later than the implementation dates for the other two components. But today, two of its rules—privacy and security—are generating a lot of discussion and debate in the health care community. The debate stems from the administrative, technical, and policy changes health care organizations are required to make to protect patients’ privacy and the confidentiality of their PHI.

Who is covered?
HIPAA states that most providers, clearinghouses, and health plans, referred to as “covered entities,” must comply with its regulations. The definition of a covered entity includes most clinical research sites (see section 160.103 of the Privacy Regulations). That means most researchers now have the additional, formal responsibility of protecting the confidentiality of PHI.

In many situations, particularly those in which the site investigator is also a clinical practitioner and in private or hospital/group practice, multiple organizations involved in research are covered by HIPAA—for instance, both the practitioner’s office and the hospital to which he or she admits patients.

**Back to basics**

The administrative simplification portion of HIPAA deals with four specific areas, but this book will not examine the billing and coding aspects of HIPAA, so that we can get to the heart of what researchers need to know to be in compliance. The three major research hot spots include:

- Privacy regulations
- Proposed security regulations
- Proposed unique identifier regulations

**Privacy regulations** govern the way a facility deals with patient or participant health information. These regulations became effective in April 2001, but entities have until April 14, 2003, to be in full compliance. Small health plans are the exception to this rule. They are not required to be fully compliant until April 14, 2004. The privacy rule protects an individual’s right to control access to and disclosure of his or her PHI. This is quite possibly the single most important aspect of the regulations for those conducting clinical trials.

**Proposed security regulations** require organizations to control the means by which PHI remains confidential, dealing specifically with electronic data transmission by computer. Since privacy requires security, the security regulations were established to complement the privacy measures. Under the security regulations, researchers have an important role in ensuring that records and data containing PHI are safe. In addition to following the previous standard procedures for storing study records in locked files, researchers must now use secure procedures with handheld and laptop computers, as well as mainframe computers and computer files that contain PHI.

At the time this is being written, these security regulations were not finalized, and HHS further delayed the release of the final version beyond the end of 2002. This portion of the act could prove costly for an institution and its research staff in more ways than fines or jail time if compliance mandates are not met. The security measures could mean replacing computer systems or replacing and updating software if a covered entity’s hardware and software technology is not up to meeting the demands set forth in the regulations.
Proposed unique facility and provider identifier regulations were first published in 1998 and final versions of the regulations are expected to be published in early 2003. Under this portion, each covered entity will have one assigned identifier number for submitting claims to all health plans and payors, eliminating the need for the multiple identifiers currently in place.

How will research be affected by HIPAA?

HIPAA does not differentiate between types or categories of research, so determining what research is covered under this law is fairly straightforward. All research performed on humans in or by a covered entity will be regulated under HIPAA. The regulations apply to treatment/research and nontreatment relationships with patients, so for anyone involved in a research project that has any contact with research participants, patients, or PHI, HIPAA will become a part of the working world.

The documentation burden

One of the key concerns—and a legitimate one—with regard to HIPAA is an increased documentation burden. If an operation is already well structured, the added workload shouldn’t be much trouble. It may be a matter of adding a half page to research consent forms to cover language specific to HIPAA. Or it may involve updating IRB protocol policies and procedures, but not rewriting the book on research if you’ve been running a tight ship all along.

Whether or not an institution has always been up to snuff in dealing with confidentiality in research, there still will be aspects of HIPAA that will be new. Some of the extra documentation will include:

- Additional “Authorization for Research” forms, or perhaps incorporating HIPAA authorization elements into current documents.
- New requirements for documentation of “pre-screening” activities.
- Different requirements for waivers and alterations of authorization.
- New requirements for documentation of pilot studies.
- New requirements for documentation of decedent research (i.e. research with PHI of the deceased).
- Retention of research authorization forms for a minimum of six (6) years.
- Applying the “minimum necessary” rule, which runs throughout HIPAA. In a study involving autho-
The minimum necessary rule amounts to telling the research subject and/or IRB what personal information will be used.

**Deadlines**

When HHS issued the HIPAA regulations in 1996, it knew what the health care industry was up against, so it gave institutions time to learn the rules and apply them to existing practices.

The major deadline covered entities face is April 14, 2003, which is when all aspects of the privacy regulations must be in place and compliance will be enforced. Until this time, compliance has been more or less optional: Covered entities were supposed to be adhering to the rules, but if they didn’t, no penalties would be imposed. But now, HHS (through the OCR) scrutiny and civil/criminal penalties await institutions that fail to address and comply with the regulations.

The next deadline arrives April 14, 2004, by which time all “business associate” contracts must be in place.

---

**Figure 1.1  What counts as Identifiers?**

Here are some examples of data that will be considered direct and indirect identifiers under HIPAA:

- Names
- Addresses
- Employers’ names or addresses
- Relatives’ names or addresses
- Dates (except year)
- Telephone and fax numbers
- E-mail addresses and personal Web sites
- Social Security numbers
- Medical record numbers
- Certificate numbers, including device serial numbers for implants
- Membership or account numbers
- Voiceprints
- Fingerprints
- Full-face photos and comparable images
- Any other characteristics that may be used, individually or in combination, to identify the individual

Determining what constitutes identifiable information may have been tough before, but HIPAA provides clear guidelines to help covered entities avoid potential trouble. If there is any doubt as to whether an identification could be made based on a piece of information, then that information should be kept private, out of respect for the patient/participant—and the law.
Business associate contracts constitute a significant administrative hurdle for providers under HIPAA, so once basic compliance is instituted and maintained, covered entities surely will turn their attention to shortening up these business associate agreements.

**Definitions**

Although HIPAA may be a useful tool for research institutions, it doesn’t come without its difficulties. The good news is that it will standardize the way facilities deal with PHI and give investigators a boost by creating a formal way to make information de-identifiable and available for research without federal or state oversight. (De-identification is covered in Chapter 8.)

However, the bad news is that the act was written in medical language, interwoven with legalese, which makes the regulation tough to follow without both a medical dictionary and a lawyer in attendance. A few of these medical-legal terms will be used throughout this book. Understanding these terms can be a key to understanding the regulations, thereby helping covered entities achieve compliance. Among the commonly used terms are:

- Research
- Minimum necessary
- Use
- Disclosure
- Individually identifiable health information
- Protected health information
- Designated record set
- Business associate
- Covered entity
- Authorization
- Informed consent
- Pre-screening
- De-identification
- Limited data set

**Research** is defined in HIPAA as “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizeable knowledge.” Hence, any kind of study conducted in a covered entity on a human—living or dead—that meets the definition of research is therefore covered under HIPAA. This is the same definition used in the Common Rule (45 CFR 46). HIPAA now
IntroduCtIon to HIPAA

brings the dead into the realm of research in its definition of “individual.”

**Minimum necessary** is the smallest reasonable amount of information needed to accomplish the activity to be performed. A facility’s IRB generally relies on the researcher to determine the minimum necessary for research purposes. The preamble to the regulation says an IRB may rely on the researcher to state his or her minimum necessary, but the rule doesn’t give any further guidance in the matter, so it may wind up being specific to the covered entity. IRBs are expected to take the PHI request at face value and seek scientific justification to use (and, particularly, to disclose) direct identifiers.

**Use** is the dissemination of information to individuals under direct control of the covered entity, even if the individual is not an employee. Here, HIPAA means the workforce of the covered entity, which includes employees and students, as well as volunteers and some on-site contractors. For example, if the facility contracts with a temporary employment agency for secretarial services on site, any information transmission involved would be considered a use.

**Disclosure** involves an activity in which PHI is given to someone who is not part of the covered entity or its workforce. For example, information given to an off-site dictation service would constitute a disclosure.

**Individually identifiable health information** is health information that identifies an individual, or upon which there is a reasonable basis to believe that the information can be used to identify an individual. The information also

- includes demographic information collected from an individual
- is created or received by a health care provider, health plan, employer, or health care clearinghouse
- relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual

**Protected health information (PHI)** is any individually identifiable health information relating to the past, present, or future health of an individual, when held by a covered entity. This is a key component of the HIPAA privacy regulations, as it relates directly to use and disclosure. Unlawful use or disclosure of PHI can result in the penalties created under HIPAA, which are covered in Chapter 2.

**Designated record set** involves a group of records maintained by or for a covered entity that may
include medical records and billing records maintained by or for a covered health care provider, and enrollment, payment, claims adjudication, and case or medical management record systems used, in whole or in part, by or for the covered entity to make decisions about individuals.

The term “record” means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

A **business associate** is defined as a person or organization that performs or helps with any activities regulated by HIPAA — such as claims processing and submission, data analysis, or quality assurance/quality improvement — on behalf of your facility or the organized health care arrangement in which your facility participates.

A business associate also may include any person or organization to whom you disclose individually identifiable health information, and who provides services such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity. Employees are not considered business associates.

A covered entity may be a business associate of another covered entity, depending upon the activities each performs. For example, a hospital that provides specialized laboratory tests to a local clinic is a business associate of the clinic.

Clinical trial sponsors are typically not business associates, as their activities are not done for, or on behalf of, the covered entity.

**Covered entities**, under HIPAA, are health care providers, health plans, and health care clearinghouses that transmit health information in electronic form in connection with a billing transaction. Basically, covered entities are the organizations that have to comply with HIPAA.

**Consent for research or research informed consent** is the process by which a patient gives his or her informed consent to take part in a research study, after being made aware of all foreseeable benefits and risks of the test article, drug, treatment or procedure, and appropriate practices within a covered entity concerning PHI.

**Pre-screening** is the process of determining which patients or persons would be potential subjects for a clinical study or research project.

**De-identification** is the process of removing all information from PHI that could be used to identify a
participant. De-identified data are not subject to HIPAA and can be used on an unlimited basis for future research or other activities. De-identification is covered further in Chapter 8.

A **limited data set** is a collection of information that does not directly identify an individual. It gives researchers as much information as they need without revealing most identifiers of the individual. Unlike de-identified data, a limited data set can only be used for research, operations, or public health purposes.

A **data use agreement** is used with a limited data set to protect the individuals from being re-identified or contacted.
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. If you received a special offer or discount source code, please enter it below.

<table>
<thead>
<tr>
<th>Title</th>
<th>Price</th>
<th>Order Code</th>
<th>Quantity</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$</td>
</tr>
</tbody>
</table>

**Your order is fully covered by a 30-day, money-back guarantee.**

- **Enter your special Source Code here:**
- Name
- Title
- Organization
- Street Address
- City  State  ZIP
- Telephone  Fax
- E-mail Address

**BILLING OPTIONS:**
- [ ] Bill me  [ ] Check enclosed (payable to HCPro, Inc.)  [ ] Bill my facility with PO # 
- [ ] Bill my (✓ one):  [ ] VISA  [ ] MasterCard  [ ] AmEx  [ ] Discover

**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.

(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

© 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