HIPAA RESOURCE GUIDES

# HIPAA DEMYSTIFIED

## HIPAA Compliance for Mental Health Professionals

LORNA HECKER, PH.D.

# PRAISE FOR HIPAA DEMYSTIFIED

"HIPAA compliance is so much more than just passing out the Notice of Privacy Practices at the first client contact. In *HIPAA Demystified*, Dr. Lorna Hecker explains the essence of the Health Insurance Portability Accountability Act of 1996 and translates it in an understandable manner, allowing readers smooth implementation of the regulations to their practices. Each chapter is arranged with clarifying 'demystification' summaries that explain HIPAA requirements in actionable terms. Dr. Hecker's use of real world case examples illustrating breaches of protected patient health information reminds us how easily this can happen and how to mitigate those risks. Search no longer, *HIPAA Demystified* will be your ultimate guide to HIPAA compliance."

*Norman C. Dasenbrook, MS, LCPC*
*Practice Consultant*
*Dasenbrook Consulting*
*Rockford, IL.*

"HIPAA is becoming the standard of care for mental health, whether or not one is officially a 'covered entity'. Therefore, it is critical that all mental health practitioners, and mental health programs and agencies, understand and adhere to the standards of care under HIPAA. While maintaining confidentiality is integral to training and practice, protecting the security of information is less familiar, and there is a need for resources that address this gap in literature. *HIPAA Demystified: HIPAA Compliance for Mental Health Professionals* meets this need and is a practical and readable resource. Clearly explaining the regulations and law, Dr. Hecker leads the reader to answer pertinent questions to develop a step-by-step guide to implementing a customized compliance program. Key to providing safeguards is a risk assessment, and the book guides you in doing so. Dr. Hecker discusses many critical elements for a mental health practice, such as clarification of how a psychotherapy

note is defined by HIPAA and what other types of information are not considered psychotherapy notes. Real world examples throughout the book illustrate the complex set of Privacy and Security Rules applicable to mental health, thus helping the reader establish safeguards to avoid breaches. A model Notice of Privacy Practices is provided as well as numerous links to websites relevant to navigating the HIPAA road! Overall, this book is an extremely relevant and helpful resource for mental health professionals who strive to maintain the security of protected health information while navigating rapidly changing technologies."

*Mary K. Alvord, Ph.D.*
*Psychologist and Director, Alvord, Baker & Associates, LLC*
*Adjunct Associate Professor of Psychiatry and Behavioral Sciences at The George Washington University School of Medicine and Health Sciences, Rockville, MD*

"*HIPAA Demystified* provides a superb opportunity for professionals in an agency or corporate setting to more comprehensively assess risk. Through the understanding of changing technologies, Dr. Hecker affords readers the opportunity to more globally understand the aspects of their agency that must be scrutinized. In an agency setting, the opportunity to identify and mitigate areas of concern is truly paramount. The agencies involved in mental/behavioral health treatment often have to find creative ways to survive, thrive, and maintain revenue streams in today's insurance driven marketplace. Any seminal event can lead to devastating legal and financial consequences. Not only does this book help to identify the legal ramifications that could impact an organization of any size, but it also sheds light on the financial outcomes that could be debilitating. A thorough assessment and understanding of the necessary HIPPAA guidelines allows for an agency to avoid financial hardship brought about by the results of damaged reputation, diminished patient care, and weakened organizational and funding source partnerships.

*HIPAA Demystified* brings to light the necessity of thoroughly understanding the reach of risk assumed within an agency. Without this

book, risk through areas such as subcontractors or other extensions of business will be difficult to pinpoint. Dr. Hecker thoughtfully allows for readers to gain a comprehensive understanding of the differing types of risk and the impact associated with it. Agencies are only as strong as their weakest link, and therefore the need for training is of the utmost importance. *HIPAA Demystified* informs the necessity of training at every level of the organization. Overall, *HIPAA Demystified*, was insightful, informative, well written, and thought-provoking. A must read for any professional, from student to CEO."

*Daniel Lettenberger-Klein M.S., LMFT*
*Regional Service Director*
*Sunrise Detox*
*Alpharetta GA*

"Hecker has created a fantastic resource for new graduates and seasoned mental health practitioners alike. This practical guide to HIPAA compliance efficiently breaks down the components of healthcare privacy into palatable pieces, informing readers without overwhelming. Hecker provides contemporary examples throughout the book to illustrate the true impact of privacy breaches, bringing the importance of thorough compliance to life. *HIPAA Demystified* is the resource to keep on hand as you navigate the complexities of patient privacy in this digital era"

*Christine Borst, PhD, LMFT*
*Director of Operations*
*Center of Excellence for Integrated Care*
*Cary, NC*

# HIPAA

## DEMYSTIFIED

HIPAA Compliance for
Mental Health Professionals

**LORNA HECKER, PH.D.**

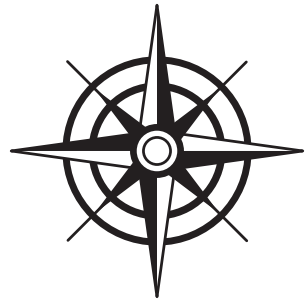
ISBN 978-1-936961-26-9

Books are available for special promotions and premiums.

For details, contact:
Special Markets
Loger Press
10769 Broadway
Suite 106
Crown Point, IN 46307
E-mail: specialmarkets@logerpress.com

Book design by Paul Fitzgerald
Published by Loger Press
www.logerpress.com
Printed in the United States of America

# TABLE OF CONTENTS



# PREFACE

Confidentiality is the ethical obligation of a mental health practitioner to keep patient information private; we respect this obligation due to our moral and professional values, ethical codes, and state statutes. Privacy is the right of clients to be free from the intrusion of others into their personal life. Both confidentiality and privacy are important foundations to psychotherapy practice. However, as we move into an era of electronic health records (EHRs), we must delve into a new area of confidentiality and privacy, which is the security of electronic records and other forms of digital data we maintain on our patients. With the advent of EHRs, the federal government realized that the public would have concerns about the privacy of this electronically kept personal health information. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was enacted, bringing federal uniformity to protecting the privacy of paper health records, as well as protecting the security of electronic health information. HIPAA gave patients[1] additional rights about the uses and disclosures of their private health information, as outlined in the familiar Notice of Privacy Practices, typically given on a patient's first visit. But what is HIPAA beyond this notice? Many practitioners are still confused about HIPAA requirements. This is understandable given there are over 1,500 pages of HIPAA regulations, detailing privacy requirements, security requirements, and electronic data interchange requirements. The advent of the Health Information Technology

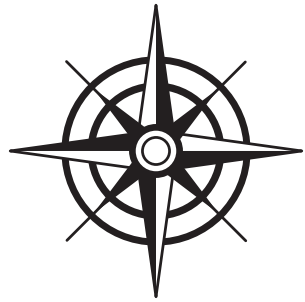
for Economic and Clinical Health (HITECH) Act, enacted in 2003, brought even more requirements including breach notification regulations.

There are some regulations of which most mental health practitioners have limited knowledge. Here are a few for you to check your knowledge base:

- Do you understand the HIPAA definition of psychotherapy notes?
- Have you completed a security risk assessment and produced a remediation plan based on the results?
- Do you understand what is required of you if a patient asks for an accounting of disclosures?
- Do you understand the difference between a designated record set and a legal record set?
- Have you designated a privacy official and a security official in your practice?
- Have you integrated stricter state standards[2] into your Notice of Privacy Practices?
- Do you understand the process of breach, a risk analysis in the event of a breach, and breach notification requirements?
- Have you instituted a workforce sanction policy, detailing potential consequences for HIPAA violations?
- Do you have a way to stay abreast of recent HIPAA developments, such as the 2013 revision requirements for your Notice of Privacy Practices?

If you can answer these questions affirmatively, congratulations, you are ahead of the curve! If you thought having a Notice of Privacy Practices and HIPAA-compliant software made you compliant, you have a ways to go. This book will help you take stock of your HIPAA compliance, demystifying the requirements such that you can more readily adapt them in your practice. Additionally, you will find case scenarios on breach of protected

health information based on actual cases such that you can learn from the mistakes of others. After reading this book and implementing the regulations that apply to your practice, you will be much more confident in pronouncing to your patients that you are indeed in compliance with the regulations.



# CHAPTER 1

## Introduction to HIPAA Compliance

While mental health professionals are intimately familiar with patient confidentiality,[3] security of patient information in the digital arena has been limited or ignored. Yet, patients are rightfully concerned about the security of their health information remaining private and secure. Identity theft of personal information may result in criminals opening new telephone service accounts, credit cards, loans, checking and savings accounts, and online payment accounts. Medical identity theft is increasing with stolen identities used to procure medical treatment, services, and supplies. Additional dangers may lurk when a patient's records later reflect incorrect medications or medical conditions.[4] Thieves have been known to give stolen identity information to law enforcement when they are stopped or charged with a crime; rent housing; obtain government benefits; or obtain employment, medical or mental health treatment, services, or supplies.[5] Tax fraud is also of concern. The digital tsunami of the past few decades has not been met with equal force in protection of our most personal data. Mental health professionals who value confidentiality must also learn to value security of the electronic health data they collect on patients in order to keep patient trust.

**History and Purposes of HIPAA**

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 with two general purposes. The first was to ensure that individuals could maintain health insurance between jobs (portability), and the second was designed to ensure privacy and confidentiality of patient health information (accountability). Under Title II of HIPAA, Administrative Simplification, the government addressed this accountability by developing privacy and security regulations. The Privacy Rule requires appropriate safeguards to protect privacy of health information and sets limits and conditions on the uses and disclosures that may be made of an individual's health information.[6] The Privacy Rule was created to lessen inappropriate disclosure of Protected Health Information (PHI) and give individuals increased control over their PHI. The Security Rule protects an individual's Electronic Protected Health Information (EPHI), providing safeguards to protect the confidentiality, integrity, and security of that digital data[7] that is created, received, used, or maintained by a provider.

Title II of HIPAA, Administrative Simplification, is directly applicable to psychotherapy practice. It includes the Privacy and Security Rules, as well as standards around electronic data interchange. In 2009, the American Reinvestment and Recovery Act (ARRA) brought the Health Information Technology for Economic and Clinical Health (HITECH) Act, which strengthened HIPAA. HITECH established breach notification rules, increased restrictions on disclosures of PHI, gave patients more rights regarding their PHI, increased fines and established criminal penalties for violations of HIPAA regulations, and provided certain other restrictions. HITECH also brought resources for compliance audits, which as a result are occurring more frequently.

*Protected Health Information (PHI) is any health information that can be used to identify a patient, who relates to physical or mental health, relating to a past, present, or future condition, and includes both living and deceased patients.*[8] *PHI may be in any form: Oral, paper, or electronic (transmitted and maintained).*

**Compliance with HIPAA Regulations**

HIPAA compliance means that you have followed the HIPAA and the HITECH Act federal regulations set by the Department of Health and Human Services (HHS) and enforced by the Office of Civil Rights (OCR). Many companies promise HIPAA compliance, yet there is no such thing; HHS does not grant compliance to entities or companies. Software vendors and others cannot apply for approval and become "HIPAA compliant." The reality is you must manage your ongoing compliance with the entirety of the privacy and security regulations consistently over time. This requires knowledge of the regulations, acquiring and applying updates when the regulations change, keeping up on evolving technology and weaknesses of your current technology infrastructure, ongoing training for your workforce, and so on. The goal of HIPAA compliance is to protect the privacy and security of your patient's private, confidential information, including any spoken, written, and electronic information.


Companies that promise you HIPAA compliance are not being entirely candid. The truth is, compliance efforts to protect the privacy and security of patient protected health information are ongoing. For example, your vendor cannot rely on an accrediting agency to certify that they are HIPAA compliant or certify that no one would be able to hack their system. It is your responsibility to assess their level of compliance under the HIPAA regulations and the level of risk you are taking on through the use of their service. Only you can create privacy and security for your clients through ongoing efforts to safeguard protected health information.

**Noncompliance with HIPAA Regulations**

Violations of HIPAA regulations are, unfortunately, commonplace. The extent of HIPAA violations ranges from unintentional disclosure to willful disclosure for personal gain (i.e., criminal enterprise). HIPAA violations largely went unpunished until the HITECH Act of 2009 clarified fines and penalties for HIPAA violations. The OCR, the branch of the HHS that investigates HIPAA violations, began compliance audits and began instituting fines and penalties for violations. Noncompliance means not following the regulations, which can result in a breach of PHI. *Breach* refers to the acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the PHI. Certain breaches of PHI result in the OCR levying fines; penalties may be brought through the Department of Justice. Breaches may even garner news coverage due to breach notification rules. For large breaches, patients must be notified, news media must also be notified, and details of the breach must be posted on the organization's website. Covered Entities (CEs) must self-report breaches to HHS; Business

Associates (BAs) must self-report breaches to the CE who contracted them. Failure to self-report can be seen as "willfull neglect," which results in additional fines. Because of these reporting measures, we are increasingly hearing about breaches of PHI. Public notifications, fines, penalties, and audits have all pushed breach of PHI to the top of the news.

The amount and depth of PHI breaches is staggering. In 2015, hackers stole PHI of 8.8 to 18.8 million people by hacking the database of Anthem Blue Cross Blue Shield.[9] Shortly after the Anthem breach, Premera Blue Cross was hacked, breaching the personal and health data of 11 million members.[10] While mental health information was surely included in these breaches, stand-alone mental health organizations have also seen significant breaches and fines. A few examples include the following:

- The nonprofit community mental health center Aspire Indiana lost the health data of 45,000 patients after several laptops were stolen from their offices.[11]
- A company laptop and hard drive of Arizona Counseling and Treatment Services were stolen from an employee's home, resulting in the loss of health data of more than 500 patients.[12]
- Compass Health, a behavioral health organization in Washington, lost a laptop containing PHI including clinical data.[13]
- The HMO Harvard Community Health Plan had electronic notes of psychotherapy sessions available in its database to which all employees had access.[14]
- Comprehensive Psychological Services in South Carolina had a laptop stolen, which included psychological records and custody evaluations.[15]

**Fines and Penalties for Noncompliance**

There are four categories of HIPAA violations that reflect increasing levels of culpability, paired with four corresponding tiers of penalty

amounts. Fines range from $100 to $50,000 per violation with a $1.5 million cap for all violations of an identical provision in a calendar year. If violations resulted from "willful neglect," which is conscious, unintentional failure, or indifference to the obligation, there are mandatory fines of $10,000 to $50,000. Offenses committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm have the highest fines and terms of imprisonments. Criminal penalties may include fines and/or imprisonment from one to 10 years, dependent upon the level of mal-intent.


DEMYSTIFIED

Costs of noncompliance with HIPAA regulations can include fines and penalties from the Department of Health and Human Services, but also include other types of financial losses, reputational damage, ethico-legal costs (e.g. harm to patients, legal liability), and damage to the therapist–patient relationship. You can spend far more in direct and indirect costs than you will on compliance efforts! Additionally, intentionally ignoring the regulations requires mandatory fines ranging from $10,000 to $50,000. Using protected health information for nefarious purposes can also garner jail time. Table 1.1 and Table 1.2 summarize civil and criminal penalties.

There are four categories of violations that reflect increasing levels of culpability and four corresponding tiers of penalty amounts that increase the minimum penalty amount of $1.5 million for all violations of identical provisions. Penalties are lowest if a CE did not know and with reasonable diligence would not have known about the violation. Additionally, penalties are waived for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect (e.g., ignoring the regulations).

| HIPAA Violation | Minimum Penalty | Maximum Penalty |
|---|---|---|
| Individual did not know and by exercising due diligence would not have known (and was generally diligent in following HIPAA regulations) | $100 to $50,000 per violation. No penalty if corrected within 30 days. Fees may be waived or penalties reduced by OCR. | Annual maximum of $1.5 million for identical provisions in calendar year |
| HIPAA violation due to reasonable cause (not due to willful neglect) | $1,000 to $50,000 per violation. No penalty if corrected within 30 days. OCR can waive or reduce penalties. | Annual maximum of $1.5 million for identical provisions in calendar year |
| HIPAA violation due to willful neglect (but violation remediated within the required time period) | $10,000 to $50,000 per violation. Penalties mandatory. This category of willful neglect occurs only when the violation is corrected within 30 days after the covered entity knew, or should have known that the violation occurred. | Annual maximum of $1.5 million for identical provisions in calendar year |
| HIPAA violation due to willful neglect (and is not remediated) | $50,000 minimum per violation minimum per violation. | Annual maximum of $1.5 million for identical provisions in calendar year |

Table 1.1. Civil fines for HIPAA violations (these figures represent fine schedules after February 18, 2009)

| HIPAA Violation | Financial Penalty | Criminal Penalty |
|---|---|---|
| Knowingly and wrongfully used and/or disclosed PHI | Fine up to $50,000 | Imprisonment up to one year |
| Deceptively used and/or disclosed PHI (false pretenses) | Fine up to $100,000 | Imprisonment up to five years |
| Used PHI for profit or false pretenses (with intent to use for personal gain or malicious harm or to sell, transfer, or use for commercial advantage) | Fine up to $250,000 | Imprisonment up to 10 years |

Table 1.2. Criminal fines and penalties for HIPAA violations (these figures represent fine schedules after February 18, 2009)

**Fines.** Violations of HIPAA regulations may lead to fines ranging from $100 per violation/record to $50,000 per violation, with an annual maximum of $1 million. For example:

- Anchorage Community Mental Health Services was required to pay $150,000 to the HHS after it failed to patch its data systems, ran outdated software, and had a breach of 2,743 records. HHS stated that it had failed to identify and address basic security risks.[16]
- Affinity Health Plan Inc. was fined $1,215,780 when it returned multiple photocopiers to a leasing agent without erasing the data contained on the copier hard drives.[17]
- The Alaska Department of Health and Human Services was fined $1,700,000 when it failed to take corrective action to improve its policies and procedures after a USB drive was stolen from the vehicle of an employee.[18]

**Penalties.** There is an increasing roster of individuals who are being charged with criminal penalties including fines and jail time. In these cases, the offender has mal-intent. For example:

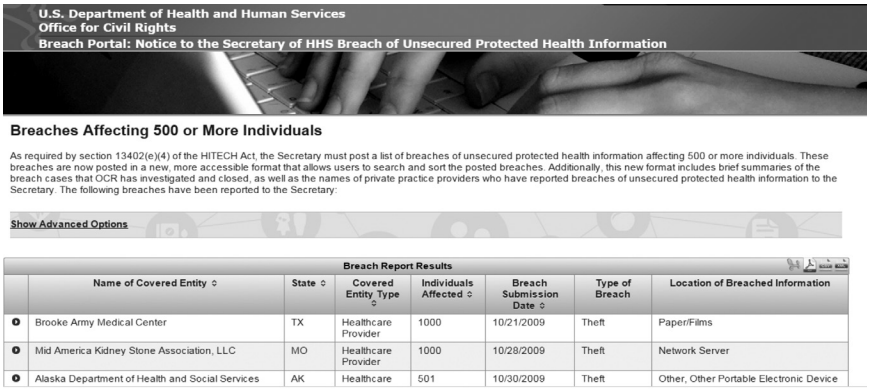
- When a doctor in Los Angeles was fired, he decided to read confidential medical records of both his supervisor and high-profile celebrities. He was sentenced to four months in prison and fined $2,000.[19]
- A nurse in Arkansas accessed a patient's file and shared the information with her husband who planned to use it in a legal proceeding. She was sentenced to two years' probation and 100 hours of community service.[20]
- A former hospital employee in Texas was sentenced to federal prison for 18 months for selling patient PHI for personal gain.[21]

**Additional Costs of HIPAA Violations**

For the average practitioner, there are additional costs for HIPAA violations. These include additional financial costs, reputational costs, legal, ethico-legal costs, and potential loss of patients due to damage to the therapeutic relationship.

**Financial.** The evolving standard practice in response to breaches is that the violating entity pays for ID theft / credit monitoring for patients whose PHI was breached. Financial loss may include image repair for public relations efforts, workforce sanctions (e.g., firing), or change in vendors when a BA is responsible for the breach. Loss may also include loss of current patients, loss of future patients, loss of customers (those who pay for services), loss of new business, and loss of staff. The American National Standards Institute (ANSI) estimates the percentage of lost revenue by the magnitude of breach. It estimates an insignificant breach costs less than 2% of revenue, a minor breach is 2% of revenue, a moderate breach is 4% of revenue, a major breach is 6% of revenue, and a severe breach will cost more than 6% of revenue.[22] The Ponemon Institute notes that costs for a data breach to be around $200 per individual record.[23]

**Reputational**. Breaches that affect over 500 individuals are to be reported to HHS and must be reported "without reasonable delay", and at the latest 60 days from first learning about the breach. Your name or your practice's name, type of breach, and number of people affected gets posted to the HHS website, to an area colloquially known as the "Wall of Shame." Additionally, patients and local media are to be notified, and breach information is to be posted on the practices' website.



U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

**Breaches Affecting 500 or More Individuals**

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results

| | Name of Covered Entity | State | Covered Entity Type | Individuals Affected | Breach Submission Date | Type of Breach | Location of Breached Information |
|---|---|---|---|---|---|---|---|
| ⊙ | Brooke Army Medical Center | TX | Healthcare Provider | 1000 | 10/21/2009 | Theft | Paper/Films |
| ⊙ | Mid America Kidney Stone Association, LLC | MO | Healthcare Provider | 1000 | 10/28/2009 | Theft | Network Server |
| ⊙ | Alaska Department of Health and Social Services | AK | Healthcare | 501 | 10/30/2009 | Theft | Other, Other Portable Electronic Device |

The HIPAA "Wall of Shame" Breach Portal[24]

**Ethico-Legal.** The requirements of the privacy and security regulations have become the standard of care for both physical and mental health professionals.[25] If your HIPAA compliance is below par, harm to patients and legal liabilities can occur. For example, when medical identity fraud has occurred, fraudulent claims may be processed, diagnoses may be delayed or inaccurate, and insurance benefits exhausted.

While there is no private cause of action written in HIPAA regulations, (e.g., you can't be sued for violating HIPAA) other types of legal action can occur in the event of a breach of PHI. You may be subject to state breach notification requirements, state consumer protection laws, or civil lawsuits for privacy violations. Under HIPAA regulations, a state's attorney general may take legal action for HIPAA violations. Accreditation bodies may also sanction your practice for violations of the regulations. Lastly, HIPAA is beginning to be used in lawsuits as the standard of care for privacy and security of PHI (*c.f. Acosta v. Byrum* [26]).

**Patient–Therapist Relationship**. Concerns about privacy also affect the therapeutic relationship. In one study, 45% of patients surveyed said they were "very" or "moderately" concerned about their medical records or insurance information being accessed without their consent. The same

survey noted that a whopping 21% of patients withheld theirs or their family's mental illness, substance abuse history, and prescription information from the treatment provider due to privacy concerns.

*"But I have a small practice—is HIPAA really important?" In 2011, Hospice of North Idaho was required to pay $50,000 for a breach of 441 records due to a stolen laptop. Upon investigation, the Office for Civil Rights found that it had not done a required security risk assessment and it had no HIPAA policies and procedures in place for mobile device security.*[27]

*Indeed, most breaches occur within small practices. Patient confidentiality no longer lies solely by guarding what you say and to whom you say it, or safeguarding paper files. The digital era has ushered in a new type of vigilance required to protect private client information, with specific parameters provided by HIPAA regulations.*

**Determining if HIPAA Applies to Your Practice**

If you practice, furnish, bill, or receive payment for healthcare in your normal course of business, or if you provide services to someone who does, you are likely bound to comply with HIPAA regulations. Individuals, organizations, or agencies that meet the definition of a CE

need to comply with the privacy and security regulations. BAs are entities that perform functions or activities on behalf of CEs, involving use or disclosure of PHI. BAs and subcontractors of BAs need to comply with the security regulations, and any contracted privacy requirements.

**Covered Entities**

A CE is any entity that transmits any information in an electronic form in connection with a transaction for which HHS has adopted a standard. Most commonly for practitioners, the main trigger for HIPAA compliance is filing for insurance reimbursement, or reimbursement from government funding entities such as medicare or medicaid. Individuals or organizations are considered CEs only if they transmit information in an electronic form in connection with a transaction as designated by HIPAA.

There are three categories of CEs: healthcare providers, health plans, and healthcare clearinghouses.

**Healthcare Providers.** Healthcare providers include doctors, clinics, mental health professionals, dentists, chiropractors, nursing homes, and pharmacies, physical therapists, rehabilitation practitioners, dieticians, occupational therapists, medical laboratory clinicians, among others.

**Health Plans.** Health plans include health insurance companies, HMOs, company health plans, or government programs that pay for healthcare such as Medicare, Medicaid, or military or veteran's healthcare programs.

**Healthcare Clearinghouses.** Healthcare clearinghouses (HCCs) are entities that receive healthcare transactions from healthcare providers or other third-party payers and then translate the data into a format that is accepted for payer(s). HCCs may also be an entity that receives this data and then processes the information into a nonstandard format, relating to claims and billing information.

**Hybrid Entities.** In addition, there is a lesser-known CE, a hybrid entity. A hybrid entity is an organization that has both covered and non-covered functions. For example, at a university a counseling center or healthcare center may meet the requirements to be a CE, but other parts of the university do not (e.g., physics, history). Those parts of the hybrid entity that provide covered functions must comply with HIPAA regulations.


If you do electronic billing *for even one patient*, you are considered a covered entity. If you subsequently opt out of electronic billing that previously triggered HIPAA, you must keep documentation of your previous HIPAA compliance for six years after the last electronic transaction.

**Business Associates and Subcontractors**

A BA is an entity or organization that creates, receives, maintains, transmits or stores PHI on behalf of a CE. Examples include entities who process claims, provide billing services, perform data analysis, or practice management. BAs may also be entities that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a CE if the service involves the disclosure of PHI. For mental health practitioners, this typically includes your billing service, answering service, attorneys, outside consultants who have access to PHI, shredding and documentation companies, and so on. A CE may also find that it is also a BA in the event that it creates, receives, maintains, transmits, or stores PHI for another CE.

BAs are required to maintain the privacy and security of PHI as provided by their business associate agreements (BAAs) or other written contracts.

With the advent of the HITECH Act of 2009, BAs are required to comply with breach notification requirements and are subject to the same civil and criminal penalties as CEs. A BA may have some interaction with your patients; they must disclose PHI when a patient or the representative requests the PHI through the CE. Due diligence must be performed to gain satisfactory assurances that a CE's BAs are complying with HIPAA regulations. BAs must assure that any of their subcontractors are also complying with the regulations.

## CASE IN POINT

Clyde's Counseling, a HIPAA covered entity, uses Betty's Billing service. Because Betty's Billing service handles receipts and billing statements, creates authorization reports, follows and verifies insurance benefits including PHI, Betty's Billing is considered a business associate under the regulations. Betty's Billing gathers a lot of protected health information paperwork in the course of business and must confidentially dispose of some protected health information from time to time. Betty's Billing hires Sam's Shredding service. Because Sam's Shredding is also handling the protected health information of Clyde's Counseling, Sam's Shredding is considered a subcontractor of Betty's Billing.

If a BA subcontracts part of its function whereby another entity creates, receives, maintains, transmits or stores PHI on behalf of a CE, the subcontractor is also subject to HIPAA security regulations, as well as any privacy stipulations set by the BA. BAs and their subcontractors are not required to name privacy officials for their organization, but must designate a security official. While BAs and their subcontractors do not have to comply with the privacy regulations, they are bound by their

Business Associate Agreements (BAAs). In these agreements, CEs will likely stipulate compliance with many of the privacy regulations. For example, if a BA keeps treatment records, and a patient wishes to amend those records, the BA must comply with this aspect of the privacy regulations. When CE requirements are discussed in this book, they typically also apply to BAs, with few exceptions.


DEMYSTIFIED

Nearly every practitioner is a covered entity, business associate, or subcontractor of a business associate, and subject to HIPAA regulations. For those few practitioners or practices that do not meet the criteria that trigger the need to be compliant with HIPAA regulations, state statutes may still cause practitioners to be subject to similar privacy and security regulations. If your practice does not meet the criteria to be a covered entity, know that many states now have breach notification laws and typically have stronger privacy statutes around mental health treatment that require vigilance to oral, written, and electronic protected health information. Case law is also beginning to establish HIPAA regulations as the standard of care for privacy and security of protected health information.

**Compliance Audits**

Lastly, the HITECH Act requires the Office for Civil Rights (OCR) to perform audits, which are increasing in frequency, even for smaller providers. Both CEs and BAs can be subject to an audit. A breach is not a prerequisite for an audit. During the first phase of audits in 2011–2012, 58 of the 59 CEs had a security finding (i.e., noncompliance). Most commonly,

CEs were simply unaware of HIPAA requirements. Two-thirds of CEs had not done the required security risk assessment; small providers (10 to 50 provider practices) struggled the most with compliance.[29] HHS is using the monies they take in from fines and penalties, in part, to further their audit efforts. Therefore, auditing will continue to increase; mental health practitioners are not immune. The audit process begins with an email from OCR asking for documentation regarding your compliance (e.g. HIPAA policies and procedures). You have 10 days to respond to the email and submit your documentation to the OCR. Your business associates may also be audited. An on-site visit by OCR may be required.

**Summary**

HIPAA was created in 1996; Title II, Administrative Simplification, affects most practitioners. Title II brought forth privacy and security regulations. CEs are required to follow the privacy and security regulations. BAs are required to follow the security regulations, and any privacy regulation stipulations set by the CE. HHS is responsible for overseeing implementation of HIPAA regulations, while the OCR is responsible for enforcing the privacy and security regulations. Noncompliance with HIPAA regulations can bring fines and penalties, with further consequences such as financial, reputational, ethico-legal problems, and damage to the therapist–patient relationship. HITECH funding for compliance audits is increasing the amount and frequency of audits, including for mental health practitioners. The purpose of this book is to guide mental health practitioners who are CEs and BAs (or their subcontractors) through HIPAA regulations to increase HIPAA compliance, thereby increasing patient confidence in the privacy and security of their personal information in which they entrust you, their provider.