THE HIPAA COMPLIANCE KIT

UNDERSTANDING AND APPLYING THE REGULATIONS IN PSYCHOTHERAPY AND COUNSELING PRACTICES

READY-TO-USE HIPPA FORMS
Available in this kit for you to personalize

By: Ofer Zur, PhD

www.zurinstitute.com

TABLE OF CONTENTS
HIPAA COMPLIANCE KIT, 10th EDITION

Form XI: Acknowledgment of Receipt of Notice of Privacy Practice
Form XII: Breach Assessment
Form XIII: Authorization to use unencrypted e-mail & text
Form XIV: Patient's Right for Confidential Communications
Form XV: Patient request for restriction on use and disclosure of PHI

References

THE HIPAA COMPLIANCE KIT: UNDERSTANDING AND APPLYING THE REGULATIONS IN PSYCHOTHERAPY AND COUNSELING PRACTICES

Tenth Edition, 2022

This HIPAA Compliance Kit aims to help psychotherapists, primarily those in solo and small group private practice, to become compliant with HIPAA regulations. The Kit provides psychotherapists with a basic understanding of the regulations and offers practical ways to achieve compliance. Sometimes simplicity and clarity for a basic understanding come at the expense of providing all the available information on a certain topic. The Kit is not meant to address every topic related to HIPAA but only highlights the most common issues mental health therapists face. The Kit is not meant to be a definitive guide to HIPAA nor does it cover how HIPAA regulations affect or do not affect specialized practices, such as those that focus on forensics, custody evaluations, education, or psychological testing or that focus on Medicare, Medicaid, or Workers' Compensation. The Kit does not provide the state-by-state preemption analysis, which is available via state boards and national professional organizations. The Kit also not a legal document or a technical manual for computers, emails, texting, or video-conferencing. HIPAA regulations are complex and still being clarified by the U.S. Department of Health and Human Services (HHS). Therefore, therapists must continually educate themselves on HIPAA regulations through a variety of sources.

Psychotherapists are permitted modify the forms included in the Kit to suit their own personal and professional needs. Forms as a Word document can be found here. They may simply copy and paste the forms into their computer and then insert their letterhead, name, or any other changes that apply to their setting and practice. Therapists should be sure that they comply with the legal, ethical, and clinical regulations of their profession and state as they adapt these forms for their own use.

Disclaimer:

This Kit does not intend to be a substitute for legal, ethical, or clinical advice or consultation. State laws may supersede HIPAA regulations and you must check with the laws and regulations of your state and your professional association. The very latest revision of the federal regulations may not be included in this Kit.

The Kit intends to give psychotherapists a basic understanding of HIPAA regulations and is not intended to provide a complete compliance manual. It is not intended to serve as the ultimate or definitive guide to HIPAA regulations. It does not provide a state-by-state preemption analysis. It does not contain details for performing a security risk analysis or for securing any given set of computers and other electronic devices.

Additionally, many regulations undergo episodic changes, and this Kit may not reflect all of the changes contained in new regulation updates. State laws also change continuously, and the result will be that guidelines for your practice will change, too. Contact your professional association, an attorney, your malpractice insurance carrier, boards and other state or federal agencies for the most current guidelines and information.

Copyrights and Liability:

This copyrighted material is not to be sold, distributed, or shared by electronic or any other means. It may be used or reproduced for the sole use of the individual practitioner who purchased the Kit. The written permission of the author is required for any other reproduction, transmission, or use of the material or portion of the material.

Unless otherwise prohibited by law, neither Dr. Zur, nor Zur Institute will not be liable to you or to any other third party for: (a) any direct, indirect, incidental, special, punitive, or consequential losses or damages, including, but not limited to, loss of profits, loss of earnings, loss of business opportunities, or personal injuries resulting directly or indirectly from use of the Kit; or (b) any losses, claims, damages, expenses, liabilities, or costs (including legal fees) resulting directly or indirectly from use of the Kit. The conditions in this paragraph apply to any acts, omissions, and negligence of Dr. Zur that would give rise to a course of legal action. You agree to indemnify and hold harmless Dr. Zur and Zur Institute against all claims and expenses (including attorney fees) arising from the use of the Kit.

The Kit is provided "as is" without warranty of any kind. Dr. Zur and Zur Institute, hereby grant you a non- exclusive, perpetual, irrevocable, and non-transferable right to use the Kit in your private office or private practice. You shall have the right to copy or modify the materials in the Kit only for use in your private office or practice. You shall not have the right to sell, transfer, use it for educational purposes, or give the Kit to another individual or entity, in whole or in part.

List of Abbreviations

AAMFT American Association of Marriage and Family Therapists
ACA American Counseling Association
APA American Psychological Association
BA Business Associate
BAA Business Associate Agreement
CAMFT California Association of Marriage and Family Therapists
CAOHI California Office of HIPAA Implementation
CARES Coronavirus Aid, Relief, and Economic Security Act of 2020
CE Covered Entity
CMS Centers for Medicare and Medicaid Services
DHHS Department of Health and Human Services, United States
DSM *Diagnostic and Statistical Manual of Mental Disorders*
EDI Electronic Data Interchange
EHR Electronic Health Record
EMR Electronic Medical Record
EPHI Electronic Protected Health Information
FERPA Family and Educational Rights and Privacy Act
HIPAA Health Insurance Portability and Accountability Act of 1996
HITECH Health Information Technology for Economic and Clinical Health Act
ICD *The International Classification of Diseases*
ICD-10-CM *The International Classification of Diseases, Tenth Revision, Clinical Modification*
IP Internet Protocol
NASW National Association of Social Workers
NBCC National Board for Certified Counselors
NCC National Certified Counselors
NPI National Provider Identifier
NPRM Notice of Proposed Rulemaking
NPS National Provider System
OCR Office for Civil Rights
PHI Protected Health Information
PMS Practice Management Systems
SSN Social Security Number
TPO Treatment, Payment, and Health Care Operations

Section I

History and Essential Features of HIPAA

What is the Health Insurance Portability and Accountability Act of 1996 (HIPAA)?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that was designed both to streamline the healthcare system through the adoption of standards for transmitting electronic health care and to help more Americans (particularly those between jobs) maintain health care coverage. Over the years, the first objective has been expanded and strengthened, while the second has been essentially lost and unachieved. From a practitioner's point of view, the heart of HIPAA regulations is patient privacy and autonomy as well as storage, retention, integrity, and transmission of records.

HIPAA is becoming the **standard of care** for security and privacy by which all psychotherapists will be judged, regardless of their billing practices. In general, HIPAA preempts state laws that conflict with its federal regulations. However, HIPAA does not preempt any state law or professional guideline that is more stringent or restrictive or that offers more patient autonomy.

HIPAA does not intend to significantly change the way psychotherapists or counselors do business or conduct therapy nor does it create or support a national data bank for medical records. However, therapists must learn to navigate the complexities of evolving professional guidelines, state laws, and HIPAA regulations, and they should consult with attorneys as necessary. [See "HIPAA Compliance Checklist" at the end of this Kit.]

What is scalable compliance?

Scalable compliance means that HIPAA requirements are size-sensitive. Large corporations (e.g., hospitals, large clinics) have many more administrative and financial burdens and responsibilities than small or one-person operations. Compared to larger operations, solo practitioners in private practice will have to do much less to become compliant but may encounter higher risks for privacy breaches because they often do not have an informed privacy expert or security information technology person on staff. All practices should consider which consequences are likely to befall them in a typical data breach.

What are the basic requirements for HIPAA compliance?

Basic requirements for HIPAA compliance include the following issues that will be discussed in detail in this Kit:

(1) a working knowledge of HIPAA regulations and updates, with legal consultation as necessary,
(2) designation of Privacy Officer and Security Officer, often the solo practitioner,
(3) creation of a HIPAA file in which documentation, procedures, and general checklists, and breach assessment analyses are kept (this "folder" may also be digital),
(4) HIPAA forms that comply with state preemption analysis and professional requirements (see sample forms at the end of the Kit that can be adapted to comply with state preemption analysis and professional requirements),
(5) management of privacy and security issues (such as virus protection, frequent computer backups, data encryption, firewalls, strict passwords, two-factor authentication),
(6) careful consideration of keeping separate clinical notes (i.e., psychotherapy notes) for some clients,
(7) posting public notices regarding the Privacy Officer and the Notice of Privacy Practices in the office and on the website, if applicable,
(8) signed Business Associate Agreement HIPAA contracts with all third parties (especially Cloud services) that manage patient information,
(9) risk analysis that is updated on a regular basis (preferably annually),
(10) maintenance of a Policies and Procedures Manual, and
(11) ongoing staff training, along with documentation about training and updates, as defined in and informed by the Policies and Procedures Manual. Although there are no specific guidelines, HIPAA training on an annual basis is considered good practice. Training should take place more often as new staff are added to the practice or as policy and procedure changes are initiated. Therapists should defer to their professional organization for guidance regarding the frequency of training.

Can HIPAA compliance be registered or documented in a standard way?

There is no registry for HIPAA compliance and no one standard way to document knowledge, risk assessment, risk analysis, or training. Ultimately, therapists' actual practices, documentations, and forms as described in this Kit will provide the evidence of compliance in the event of a random audit or a formal complaint.

How is HIPAA compliance audited, and how are formal complaints addressed?

The Office for Civil Rights within the U.S. Department of Health and Human Services conducts random audits that include explanations of the process and that are generally not meant to result in punishment or remediation orders. However, in cases where therapists are way out of compliance, random audits can result in a formal compliance review which does have the potential for remediation and punishment.

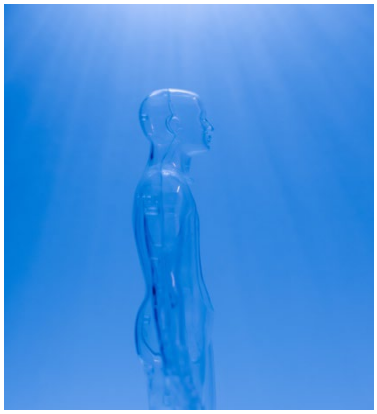
In addition, any person (a patient or otherwise) who believes that a therapist is not complying with HIPAA regulations may file a complaint with the Office for Civil Rights, and, once the complaint process unfolds, the therapist's entire operation will be under scrutiny. HIPAA does not allow for therapists to segregate that part of their practice to which HIPAA standards apply.

What changes have been made to HIPAA over time?

HIPAA is the result of the Kassenbaum-Kennedy bill that was signed into federal law by President Bill Clinton on August, 21, 1996. Since then, the Department of Health and Human Services (HHS) has issued five major updates to HIPAA to protect patients' health information, namely through the **Privacy Rule (2003), Security Rule (2005), The Final Breach Notification Rule (2009), The Transaction Rule (2009), and the Omnibus Final Rule (2013).**

The Final Breach Notification Rule (2009) and the Omnibus Final Rule (2013) stemmed from the **Health Information Technology for Economic and Clinical Health Act (HITECH Act)** that was signed by President Barack Obama in 2009. As part of the American Recovery and Reinvestment Act, the HITECH Act incentivized the adoption and use of health information technology and further strengthened HIPAA. As a result of the HITECH Act, the Office for Civil Rights issued a **Notice of Proposed Rulemaking (NPRM)** in 2020 that proposed many changes to the HIPAA Privacy Rule. In addition, the Office for Civil Rights began issuing HIPAA-compliance audits and established tiered financial penalties for noncompliance. The consequences of not being complaint with HIPAA can be costly and significant. Civil and criminal penalties are applied to Business Associates as well. Lawsuits from patients are always a possibility if therapists are noncompliant and patients' health information is not adequately protected.

Section II
The Privacy Rule



How are protected health information (PHI) and electronic protected health information (ePHI) defined?

The HIPAA Privacy Rule guards all **protected health information (PHI),** including individually-identifiable physical or mental health information, regardless of format (e.g., handwritten, electronic, oral statements). In the field of mental health, PHI is similar to what constitutes confidential psychotherapy (medical) records and is defined as any individually-identifiable information that relates to a patient's mental health condition, the healthcare of such an individual, or payment for the healthcare. Health records, health histories, lab results, and medical bills are considered PHI. PHI also includes any information that identifies the patient or that could reasonably be used to identify them (e.g., using their initials). Data such as names, telephone numbers, Social Security numbers (SSN), email addresses, medical record numbers, account numbers, full-face photos, retinal scans, and fingerprints constitute PHI. PHI includes not only past and present health information but also future health information, such as medical prognoses and treatment plans. The definition of **electronic PHI (ePHI)** is the same as PHI but specifically refers to information that is transmitted or maintained in electronic media, stored digitally, or is part of electronic networks of any kind.

PHI excludes Individually Identifiable Health Information in educational records covered by the Family and Educational Rights and Privacy Act (FERPA). Financial institutions have a special exemption from HIPAA, so therapists are not expected to apply HIPAA's standards to the most basic payment processes, such as running debit or credit cards or depositing checks. The Privacy Rule does not restrict release of de-identified health information for which any identifying information has been released. Examples include removing names, birth dates, or any other types of information from which a patient can be recognized. De-identified health information is not considered PHI because it no longer contains individually-identifiable information.

What is the primary purpose of the Privacy Rule?

The primary purpose of the Privacy Rule is to limit and define the circumstances under which a person's protected health information may or may not be shared. The Privacy Rule focuses on the application of effective policies, procedures, and agreements to

protect privacy through the control, access, and use of medical records. To this end, it requires psychotherapists to inform all patients about office privacy policies and how they are implemented, make sure patients' records are not inappropriately disclosed, obtain patients' authorization or consent for sharing information for non-routine purposes (e.g., marketing), and train employees so that they understand privacy procedures.

The HIPAA Privacy Rule is designed to provide a **minimum federal standard** and does not preempt state laws if state laws are more restrictive. Most professional privacy and confidentiality safeguards are stricter than those mandated by HIPAA. Of course, HIPAA takes precedence over state laws and professional guidelines that provide less privacy protection or less autonomy for patients. In general, HIPAA privacy regulations will not significantly change the way therapists deal with informed consent and authorization to disclose protected health information.

To whom does the HIPAA Privacy Rule apply?

The Privacy Rule applies to almost all health plans and healthcare providers, including psychologists and other psychotherapists. Nearly all healthcare providers, health plans, persons, and organizations that bill or pay for health care are considered **Covered Entities (CE).** HIPAA defines a Covered Entity as a "health care provider" who "transmits health information in electronic form" as part of any "covered transaction." Psychotherapists who submit billing electronically through a billing system are considered to be Covered Entities. At face value, therapists who accept cash payments from clients, never bill insurance companies via electronic means or have their clients submit insurance claims themselves would not be considered Covered Entities. ***However, even psychotherapists who are not Covered Entities under HIPAA should seriously consider following HIPAA regulations when it comes to privacy and security, as these regulations are rapidly becoming an integral part of the standard of care.***

Business Associates (i.e., organizations or people other than a member of the therapist's office who creates, receives, maintains or transmits PHI on the therapist's behalf to provide services to, or on behalf of, the therapist) also must be HIPAA-compliant. Some examples of Business Associates include billing services, collection agencies, clearinghouses, off-site computer repair services, and transcribing agencies.

For assistance in determining whether an organization or individual is considered a Covered Entity under HIPAA, refer to the following government link: Covered Entity Decision Tool (cms.gov).

What is a Notice of Privacy Practices (NPP)?

The Privacy Rule requires therapists to provide their patients with a notice of their privacy rights and therapist privacy practices. In addition, the HIPAA notion of authorization includes certain specific elements that need to be explicitly addressed in authorization forms. The **HIPAA "Notice of Privacy Practices (NPP)"** should be mailed directly to patients upon phone intake, posted on therapists' websites and in their offices, and obtained as reasonably as is practical in emergency situations. Even if therapists already have a standard informed consent or office policies form, they still need to provide a separate HIPAA NPP form.

Therapists who are part of a group of providers and have a joint Notice of Privacy Practices may also obtain a joint consent. A joint consent must identify the Covered Entities to which the joint consent applies and meet the other requirements outlined for consents. If a patient revokes a joint consent, the therapist who receives the revocation must inform the other Covered Entities involved as soon as possible.

The Notice of Privacy Practices describes the Covered Entities and service delivery sites to which the notice applies and states that the Covered Entities will share information with one another as needed. However, most state laws preempt HIPAA on this issue and require that therapists get patients' authorization before disclosing any confidential information. [See "Notice of Privacy Practices (NPP)," "Authorization to Release Information" and "Acknowledgement of Receipt of Notice of Privacy Practice" forms at the end of the Kit.]

How can organizations use and disclose PHI?

The HIPAA Privacy Rule defines **"use"** as the sharing, employment, application, utilization, examination, or analysis of individually-identifiable health information by an entity that maintains such information. **"Disclosure"** is the release, transfer, giving access to, or divulging information to an outside entity.

Covered Entities must only disclose the **minimum necessary** amount of information needed to accomplish the intended purpose of the requestor's need, and they should not share entire medical records unless justified. When submitting information to a collection agency, therapists should only provide essential information such as name, phone number, mailing address, and account balance. No clinical information should be given to collection agencies. As has always been true for psychotherapy, getting a patient's specific authorization for disclosure and indicating the type of information is often the safe and clinically-advised route. The "minimum necessary" requirement does not apply to disclosures that are made in response to a patient's signed authorization.

Minimum disclosure guidelines do *not* apply in the following situations:

- sharing information with a health care provider to obtain treatment,
- providing information to the individual or legal representative
- providing the information requested by the individual or legal representative, and
- when required by law or when requested by Health and Human Services for enforcement, investigation, audit, or compliance review activities.

HIPAA introduced a **"need to know"** requirement in 2003 that was not covered by most state laws or professional guidelines at the time. Therapists must identify which members of their workforce need access to PHI and give them access only to the information needed to do their jobs. For example, a billing clerk should have access only to a patient's demographic and billing information, not the patient's entire psychotherapy record.

Covered Entities may *not* share protected health information with others, except as the Privacy Rule allows or requires, unless authorized by the person or the person's legal representative to whom the data is in reference. In addition, Covered Entities must provide access to protected information to individuals or their legal representatives unless there are permitted grounds for denial. Finally, Covered Entities must explain their disclosure of protected health information to the protected individuals or their legal representative when requested. [See "Patient's Requests for Restriction and Termination of Restrictions on Use and Disclosure of PHI" form at the end of the Kit.]

Covered Entities may generally share protected health information without the authorization of the patient under the following circumstances:

- to provide treatment, including but not limited to consultations, referrals, coordination, and management of healthcare. For example, a psychologist may share patient health information when referring a patient with depression to a psychiatrist to be evaluated for medication. However, many state laws and professional guidelines require patient authorization in these cases and preempt HIPAA.
- to provide treatment when the patient is an unemancipated minor or an adult who has a legal guardian or healthcare surrogate. Parents and guardians are considered the personal representatives and, therefore, can access PHI, excluding psychotherapy notes. Special rules dictate the sharing of information in certain circumstances (e.g., cases in which children are victims of abuse by the parent or the patient is receiving services through a federally-funded drug and alcohol abuse treatment program).
- to obtain payment or receive reimbursement for healthcare services provided to the individual. For example, a psychologist may share the information needed to receive compensation from a client's private health insurance company.

- to perform healthcare operations, including quality assessment and improvement, medical reviews, audits, performance evaluation, accreditation, credentialing, business planning, management, insurance functions, legal services, and competency assessment. For example, psychotherapists may and should share information when state surveys are conducted to determine a facility's compliance with regulations.
- when required or authorized by statute or regulation, such as when there is imminent severe danger. Psychologists are bound by a "duty to warn" in order to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Therapists may disclose PHI without authorization to someone reasonably able to prevent or lessen the threat. Such a disclosure can be made to the person who is threatened. HIPAA regulations regarding disclosure in the case of threat or danger are generally consistent with most states' existing "duty to warn" laws.
- when a patient is in an emergency or is incapacitated, provided that the sharing of information is in the patient's best interest as determined by the healthcare provider. Limitations may include the client's name, location in the facility, and necessary information about the person's condition. For example, the psychologist may tell family or friends specific information if a client is confused and unable to grant consent if the psychologist deems that sharing the information is in the client's best interest. Additional protections exist for clients who are in substance abuse treatment programs.
- when state and federal laws or court orders mandate disclosure, such as during a criminal court proceeding, subpoena, summons issued by a judicial officer, a grand jury subpoena
- for judicial or administrative proceedings if the request complies with additional rules regulating the sharing of information in those proceedings
- during health oversight activities such as government-authorized audits and investigations
- to federal and state public health authorities to prevent disease
- to governmental agencies that are assigned to receive reports of elder, domestic, or child abuse
- for enrollment in specific public benefit programs. For example, a psychologist may share PHI with a social services agency, such as a housing program, if the patient's eligibility is based on mental health issues.
- for research purposes, if the data have been de-identified (which means it no longer is considered PHI) and there is an approved waiver from an institutional review board

The Privacy Rule permits a therapist to disclose a complete PHI, including portions that were created by another provider, for the purpose of treatment. However, state laws and other professional regulations may require patients' "authorization to disclose" in these kinds of situations, and consultation with legal experts is advised.

According to HIPAA, patients' consent is not required for use or disclosure of information for **treatment, payment, or healthcare operations (TPO). Treatment** involves providing psychotherapy, consultation with other healthcare providers, and/or referral. **Payment** consists of activities related to the patient receiving care, including billing, eligibility determination, claims management, collection activities or obtaining payment under a reinsurance contract, review of health care services for medical necessity, coverage, or appropriateness or utilization of review activities. **Healthcare Operations** include quality assessment, underwriting, reviewing the competence or qualifications of healthcare professionals, premium rating, medical review, legal services, auditing and business management, and general administrative activities.

However, most states have stricter and more protective laws that preempt HIPAA with respect to TPO. Similarly, professional ethics are often stricter than HIPAA on issues of TPO disclosures. Therapists may choose to get patients' HIPAA authorization for TPO even though it is not mandated. Patients have the right to submit a written revocation of consent for TPO at any time but a revocation is not effective if the therapist already acted in reliance of it and provided the services.

How does the Privacy Rule define marketing?

The Privacy Rule defines **marketing** as the creation of a communication about a product or service for the purpose of encouraging recipients (i.e., patients, former patients, or other individuals based on diagnosis) to purchase or use that product or service. Generally, patient authorization is required before a therapist is able to use or disclose PHI for marketing purposes. For example, therapists must obtain patient authorization before sharing and selling a patient's PHI to pharmaceutical companies that, in turn, send promotional materials and coupons to patients for new psychotropic medications.

Communications that describe products or services that are included in the healthcare network are not considered to be "marketing" and do not require patient authorization per HIPAA. For example, therapists are permitted to send patients an announcement about a new specialty group or new equipment within the practice through a general mailing or publication without patients' prior authorization. Similarly, communications that are made for the specific treatment of the patient (e.g., medication refill reminders, case management, coordination of care) are not considered marketing.

As with any other HIPAA regulation, a preemption analysis with state law and professional regulations will determine therapists' course of action regarding

disclosure of information without consent, and consultation with an attorney is advised.

How does the Privacy Rule address confidential conversations?

The HIPAA Privacy Rule requires that therapists ensure that their **confidential phone conversations, answering machine messages, and voice mails** are not overheard by unauthorized people and that therapists train their staff to do the same. Therapists should get clear information from patients as to how therapists and staff can call patients and what kind of information to include in their messages to them. Therapists who provide audio-only telehealth must make reasonable safeguards to protect PHI by conducting sessions in private locations whenever possible and by using lowered voices to avoid potential that confidential information is overheard. Therapists who use transcription services must make sure that the company is in compliance with HIPAA and that they have a Business Associate Agreement. (Business Associates and Business Associate Agreements will be discussed in greater detail in the section on the HIPAA Final Omnibus Rule, 2013). Generally, HIPAA is more lenient with classic phone companies than with Voice over Internet Protocol (VoIP) services, due to security risks pertaining to the Internet. [See "Patient's Right for Confidential Communication" form at the end of the Kit.]

How does the Privacy Rule address fax machines and home offices?

PHI sent via **fax machine** must include a cover sheet with clear instructions regarding how to handle a fax that reached the wrong recipient. Therapists must keep a log of clinically-related faxes received and sent and must maintain policies as to how to keep unauthorized people from data on fax machines, how to ensure confidentiality if content is stored on unencrypted hard-drives within a combined copier, fax, and printer device, and how to thoroughly erase hard-drives when the machine is sold, discarded, or returned to a leasing company.

Therapists who have **home offices** or who bring PHI home should consider designating lockable spaces for storing devices and equipment that handle PHI. Considerations should be made for how to transport materials safely or store PHI on the Cloud in a manner that is HIPAA-compliant. Cloud services include email, some texting services, online electronic record systems, online practice management systems (PMS), online data backup systems, online document systems (e.g., Google Docs, Microsoft Office 365), eFAX services, online assessment services, and video calling services.

Section III
Records and Access

What rights do patients have over their health information?

Besides protection of patients' privacy, HIPAA is committed to enhancing patients' autonomy and access to their records and gives patients some new rights with respect to their health information. Some of the new rights include the following: (1) to receive notice about a therapist's privacy practices, (2) to restrict the use or disclosure of PHI, (3) to access health information, (4) to request amendments to health information (known as the right of notice), and (5) to obtain an accounting of the uses and disclosures of PHI.

Under what circumstances may therapists deny patients' access?

Therapists may deny a patient access to PHI provided that the patient is given the right to have the denial request reviewed. Therapists may deny access if it is reasonably likely to endanger the life or physical safety of the patient or another person. In addition, therapists may deny access if the PHI makes reference to another person (unless that person is a healthcare provider) or if such access is reasonably likely to cause substantial harm to the other person. For example, a therapist may deny access to the PHI if a friend, spouse, or lover added or called in sensitive information to the therapist.

If therapists deny a patient access to records, they must provide a timely written denial in plain language that contains the basis for the denial, a statement of the patient's review rights and how the patient may exercise review rights, a description of how the patient may complain to the provider (with name and telephone number of the compliance office or the office designated to receive complaints), and an explanation of how the patient may complain to the U.S. Department of Health and Human Services.

Patients may not have the right to access information compiled for a civil, criminal, or administrative proceeding. In addition, therapists may deny a patient access without providing an opportunity for review if the PHI is exempt from the right of access, the information is part of ongoing research, or the PHI was obtained by someone other

than a healthcare provider under a promise of confidentiality. [See "Denial of Access to Protected Health Information (PHI)" at the end of the Kit.]

What special considerations should be made for psychotherapy notes?

Patients do *not* have the right under HIPAA to view their **psychotherapy notes** (if the therapist keeps them). Psychotherapy notes may include intimate, personal details about patients, details of dreams or fantasies, sensitive information, therapists' own countertransference, and therapists' hypotheses and speculations. (Psychotherapy notes are distinct from essential information for the patient's medical record, such as medication monitoring, start/stop times of sessions, modalities and frequencies of treatment, results of clinical tests, diagnoses, functional status, treatment plan, symptoms, prognosis, and progress.) Psychotherapy notes are used exclusively for the therapist's reference and, therefore, receive special protections. They are kept separate from the medical record and from the purpose of payment, referrals, or continuity of care. Psychotherapy notes may be from any type of session, including, but not limited to, individual, group, or family counseling.

While some practices (especially more psychoanalytically-oriented ones) may choose to exercise the option of keeping two sets of records (i.e., an official medical record and psychotherapy notes), therapists generally are discouraged from maintaining two sets of records. Therapists should assume that no records, including psychotherapy notes, are immune from disclosure. Psychotherapy notes may need to be presented in specific cases, such as certain criminal proceedings.

If psychotherapy notes are recorded electronically, they should be in a separate section of therapists' notes software from other records or notes and should be clearly labeled as follows: "These psychotherapy notes are part of the record and are in compliance with HIPAA regulations. They should be kept separately from the rest of the healthcare records."

Managed care companies often argue that they own the entire record, including the psychotherapy notes. However, managed care and insurance companies do *not* have the right to review psychotherapy notes. In addition, HIPAA does not permit managed care and insurance companies to make the disclosure of the psychotherapy notes a condition of treatment. Generally, therapists may not disclose psychotherapy notes for payment purposes without a signed authorization to release from the patient.

Psychotherapy notes can be shared with other healthcare providers only if a specific authorization from the client is obtained. Specific authorization should be constructed carefully, and the fact that patients can sign such an authorization may mean that the therapists lose control over who may be able to access the information. If a patient authorizes a disclosure of psychotherapy notes to a non-Covered Entity who is also

not a HIPAA Business Associate, that entity or person may release it to whomever they wish, without any need for authorization because they are not likely regulated by HIPAA. Generally, therapists cannot disclose (or re-disclose) psychotherapy notes that were created by or received from another therapist without an authorization from the patient.

Patient's authorization is mandated for a therapist to disclose psychotherapy notes except in special situations, such as when mandated by law, when there is serious and imminent threat to the health or safety of a person or the public, for the purpose of therapists preparing a defense in legal proceedings, and to assist a coroner or medical examiner in identifying a deceased person or determining the cause of death.

What is compound authorization?

An authorization for disclosure of PHI may not be combined with any other document to create a **compound authorization** with a couple of exceptions: (1) an authorization to disclose information created for research may be combined with a treatment authorization, and (2) an authorization for disclosure of psychotherapy notes may be combined with other authorizations.

What is the time frame for a patient's request to review records, and what fees are permitted?

Under HIPAA guidelines, therapists must act on a request for access within 30 days of receipt of the request. Therapists may extend the time for an additional 30 days but must provide the patient with a written explanation for the delay. However, many state laws require that therapists respond in fewer than 30 days; therefore, a state-by-state preemption analysis ultimately determines the length of time (whichever is shorter).

Under HIPAA, therapists are required to provide the patient with records requested in electronic form, if that is the nature of the request. Therapists can impose reasonable cost-based fees for copies (e.g., cost of supplies and labor, postage) and fees for preparation of a summary of the PHI if requested. Fees may not include costs associated with searching for and retrieving the information.

What rights do patients have to amend their records?

Under HIPAA, patients have the right to request to amend their PHI if they believe it is incorrect. Therapists must act on the request within 60 days of receiving the request and a 30-day extension is permitted if the patient is given written notice. If therapists accept all or part of the requested amendment, they must make the amendment, inform the patient, ask the patient if anyone else should be notified of the amendment, and provide the information to the parties the patient identifies. All information and

communication related to granting or denying requests must be included in the patient's record.

Therapists may deny requests for amendments when the record was not created by the therapist and the creator is no longer available, when the record is not part of the designated record set, when it is not available for inspection, or when the therapist thinks that the record is in fact accurate and complete. As was the case for a denial of access to PHI, therapists who deny a patient's request for amendment must provide the patient with a timely written denial explaining the basis for the denial, the patient's right to submit a written statement of disagreement, and how the patient may complain to the privacy officer or the U.S. Department of Health and Human Services. [See "Request for Amendment of Health Information," "Denial of Request for Amendment," and "Sample Complaint" forms at the end of the Kit.]

What about records of minors?

In general, the HIPAA Privacy Rule recognizes parents or other legal guardians as personal representatives of their children and grants access to their PHI. However, HIPAA intends not to interfere with state laws regarding parental control and access to their children's mental health treatment, and state laws preempt HIPAA in most cases. There are a few exceptions to the right of parental/guardian access to minors' records, most notably when a state law allows a minor to access mental health services without parental consent, when a court makes the determination, and when a parent/guardian consents to an agreement of confidentiality between the minor and the healthcare professional. When a parent/guardian signs an authorization for the release of records, the authorization remains valid even when the child becomes an adult, until it is revoked or expires.

What are the considerations for an accounting of disclosures?

HIPAA provides patients with the right to request an accounting of disclosures that details with whom their health information has been shared. Therapists must give patients, upon request, an account for disclosures of PHI for 6 years prior to the date of the request. State and professional regulations related to the number of years records must be preserved must be taken into consideration.

The accounting must include the date of the disclosure; the name of the person or entity who received PHI and the address, if known; a brief description of the PHI disclosed; and a brief statement of the purpose of the disclosure or a copy of the written request for disclosure. A patient's first request in any 12-month period must be provided free of charge, but therapists may charge patients for an account of disclosure if the patient requests more than one within a 12-month period. Therapists must respond to the patient's request within 60 days of receiving the request, and an extension of 30 days is permitted with written notice to the patient. [See "Tracking of Releases" and "Account of Disclosures" forms at the end of the Kit.]

Section IV
The Security Rule

How does the Security Rule set standards for the protection of ePHI?

Securing computer records and electronic transmissions (e.g., electronic medical records, emails) has been one of the most basic goals of HIPAA from its inception. The HIPAA Security Rule sets the standards for the protection of PHI in **electronic format (ePHI)** that is kept in electronic media such as computers and smartphones and that is being sent across networks, such as the Internet. *(The Security Rule does not apply to PHI that is not in electronic format.)* The Security Rule also provides guidelines for therapists to make sure electronic information is not lost or deleted before intended and is not damaged or modified except when intended, and it applies to all healthcare and business associates who have access to ePHI.

The Security Rule is flexible with regard to various implementation strategies. Its text makes frequent use of the phrases "reasonable and appropriate" and "reasonably anticipated." In addition, the rules do not intend to institute security against all potential threats in the world. The key is that the therapist took reasonable steps to assess and manage risks and documented these analyses. The Security Rule is also technologically neutral, meaning that therapists can choose software or hardware that works for their practice and supports HIPAA compliance. There is no endorsement of any specific product or certain way of achieving security. HIPAA also recognizes that implementation is a work in progress, especially for rapid changes in technology.

According to the Security Rule, Covered Entities must do the following:

- protect the ePHI against potential threats to its security and integrity,
- train employees and ensure compliance with the Security Rule,

- adapt suitable policies and procedures, and
- create a risk management plan to mitigate the risk to ePHI.

The Security Rule defines some policies that therapist must have in place to physically protect their ePHI from a breach. For example, they must position their computer screens so that passersby cannot view material and store electronic equipment in places that cannot be accessed without keys or without checking in with office personnel. HIPAA also requires therapists to retain a list of people who access computers and other digital devices and know passwords. It also mandates that therapists regularly back up computer-stored information and assure that access to backups is restricted and monitored. If several people have access to a particular computer, therapists must document who they are, their job descriptions, and what aspects of data they are allowed to access.

What are some basic considerations regarding computer security?

The following are some of the most basic aspects of computer security that HIPAA requires:

- well-updated **virus and malware protection** (i.e., protection against viruses that can destroy and corrupt data and protection against malware that can gather passwords, send them to hackers, and install viruses)
- strict **password management policy** (i.e., policy that involves changing passwords regularly, maintaining a minimum password strength standard, canceling access to former employees, and never posting passwords on the computer or in the office)
- maintain an **access log** (i.e., different people should use different accounts and passwords)
- create a **separate user account** on the computer for all clinical work if the computer is also used for personal reasons and/or by other family members or make heavy use of Cloud services for PHI instead of keeping it directly on the computer
- **firewall** that protects computers from invasion by viruses and hackers and is updated as soon as new updates are available (i.e., generally built in or inexpensive and easy to install)
- **automatic logoff** after a certain amount of idle time
- regular **computer backups** to ensure no PHI would be lost if the computer were lost or damaged (i.e., encrypt backup disks and consult with experts about HIPAA compliance related to Cloud storage and other digital backup options)
- **erase information thoroughly** (i.e., ask experts for help if needed, as tossing electronic documents in the "trash" is insufficient and is potentially accessible to unauthorized people)

- **encrypt** both computer hard drives and backup disks and pair this safeguard with strong encryption passwords

What are some basic considerations for smartphones and tablets?

The above security measures should also be in place for smartphones and tablets that access and transmit ePHI, whether they are issued by the office or are personal devices. Here are some specific issues to consider for these devices:

- Although iPhones and iPads have some built-in antivirus and anti-malware software and firewall software, therapists must exercise caution about accessing websites and downloading apps.
- Most mobile devices have features that allow the user to limit wrong password guesses and lock the device automatically and immediately when they are not in use.
- Therapists also should turn off virtual assistants (e.g., Siri, OK Google, Cortana) from the lock screen and only have them available after a device is unlocked.
- Therapists also should ban PHI-containing alerts (e.g., "Joe Client sent you an email") from the lock screen and should instead change settings so that notifications are vague (e.g., "You have received an email.") so that notifications do not inadvertently cause a breach of information.
- Therapists should utilize remote tracking features. Most mobile devices can be set up so that therapists can track their location and even wipe them clean remotely. This feature must be set up on all devices and can work even when the devices are shut off as long as they have battery and are connected to the internet.
- Back up from hand-held devices to a computer that is full-disk encrypted and backed up. Cloud storage is an option but consultation with an expert is necessary to ensure the software vendor is HIPAA compliant.
- Limit or eliminate Cloud-based app synchronization (a feature under device settings). Therapists who need to synchronize apps with their own computer may do so by using a cable or office Wi-Fi.
- Consult with experts about thoroughly erasing electronic data before discarding old devices.

What considerations should be made for all electronic devices that are connected to Wi-Fi?

All electronic devices connected to Wi-Fi can interact with one another. Wi-Fi must have the following security measures to prevent devices from eavesdropping or hacking:

- Use WPA2 security with a password that is difficult to guess, and never leave the password on default.

- Only give the Wi-Fi password to people who need it for conducting the practice's business.
- Have a separate Wi-Fi for guests, including patients. Most modern Wi-Fi routers come with the ability to set up an office Wi-Fi for staff and a separate guest Wi-Fi for patients and other guests, all on one Wi-Fi router.
- If Wi-Fi is shared with other businesses in a building, therapists should establish a personal hotspot device that uses their own phone's data plan. They should make sure that their data limit is high enough to accommodate the needs of their practice. If permitted, they should use the building Wi-Fi as the Wi-Fi for patients and other guests.
- If therapists need to use devices while out and about, arrange a Wi-Fi hotspot rather than using public, unsecured Wi-Fi.

What is a Risk Analysis?

The Security Rule requires therapists to conduct a **risk analysis,** an assessment of the vulnerability and potential threats to confidential information in their practices. **Technical vulnerabilities** may involve weaknesses in the development or configuration of information systems, while **non-technical vulnerabilities** may include inadequate policies, procedures, and standards. **Threats** may be **natural** (e.g., floods, earthquakes, tornadoes, landslides), **human** (e.g., intentional threats, such as computer hacks that grant unauthorized access to PHI; unintentional threats, such as mistakes related to data entry or deletion), and **environmental** (e.g., power failures, chemical spills, pollution). After a therapist identifies areas of vulnerability and threat, he or she must assess current security measures and determine the likelihood that the threat will occur and the potential affect that the threat would have on the confidentiality and availability of patients' PHI.

A risk analysis includes:

- identifying potential risks to patient health information, ranked highest to lowest
- identifying all resources that touch ePHI,
- creating a risk management plan and reviewing on a yearly basis,
- enacting administrative, physical, and technical safeguards,
- conducting HIPAA training when relevant, and
- documenting the risk analysis process.

Based on the risk analysis, therapists are expected to develop, implement, and maintain measures to safeguard the integrity, confidentiality, and accessibility of important electronic data. The risk analysis and security plan must be documented.

Table 2: Examples of Potential Information Security Risks with Different Types of EHR Hosts[1]

Host Type	Risk	Examples of Mitigation Steps

[1] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Office-Based EHRs	Natural disaster could greatly disrupt the availability of, and even destroy, ePHI.	Always store routine backups offsite.
Office-Based EHRs	You directly control the security settings.	Regardless of your practice size, follow best practices on policies and procedures about access to ePHI. For example, use password controls and automatic logout features.
Office-Based EHRs	The security features on your office-based EHR may not be as up-to-date and sophisticated as an Internet-hosted EHR.	Maintain ongoing communication with your EHR developer about new features and their criticality to the security of the EHR.
Office-Based EHRs	When public and private information security requirements change, you have to figure out how to update your EHR and work out any bugs.	Routinely monitor for changes in federal, state, or private-sector information security requirements and adjust settings as needed.
Internet-Hosted (Cloud-Based) EHRs	You are more dependent on the reliability of your Internet connection. Your data may be stored outside the U.S., and other countries may have different health information privacy and security laws that may apply to such offshore data.	Confirm that your EHR host follows U.S. security standards and requirements.
Internet-Hosted (Cloud-Based) EHRs	The developer may control many security settings.	The adequacy of these settings may be hard to assess, but ask for specific information.
Internet-Hosted (Cloud-Based) EHRs	In the future, the developer might request extra fees to update your EHR for compliance as federal, state, and private-sector information security requirements evolve.	Ensure your EHR stays compliant. Before you buy, it is OK to ask your developer about fees it may charge for security updates.

What considerations should be made for e-mail, social media, websites, telehealth, and video-conferencing?

E-mail: E-mail signatures at the end of emails have minimal impact on HIPAA compliance but do help recipients understand what they have received and what to do if they received an email in error. The following is an example of an e-mail signature to patients:

> Notice of Confidentiality: This e-mail, and any attachments, is intended only for use by the addressee(s) and may contain privileged, private or confidential information. Any distribution, reading, copying or use of this communication and any attachments by anyone other than the addressee, is strictly prohibited and may be unlawful. If you have received this e-mail in error, please immediately notify me by e-mail (by

> replying to this message) or telephone (xxx-xxx-xxxx), and permanently destroy or delete the original and any copies or printouts of this e-mail and any attachments.
>
> It is important that the addressee/s be aware that e-mail communication can be relatively easily accessed by unauthorized people and hence can compromise the privacy and confidentiality of such communication. E-mails, in particular, are vulnerable to such unauthorized access, due to the fact that servers have unlimited and direct access to all e-mails that go through them. A non-encrypted e-mail, such as this, is even more vulnerable to unauthorized access. Please notify xxx if you decide to avoid or limit, in any way, the use of e-mail. Unless I hear from you otherwise, I will continue to communicate with you via e-mail when necessary or appropriate. Please do not use e-mail for emergencies. While I check my phone messages during the day when I am in town, I do not always check my e-mails daily.

Social Media: HIPAA does not define whether or not a presence on social media is acceptable nor does it require anything about the nature or format of a therapist's social media presence. However, HIPAA does require that therapist's risk analysis and risk management plan cover all the areas where breaches to confidentiality, integrity, or availability of PHI reasonably may be anticipated. HIPAA is not concerned about ethical issues of therapist self-disclosure or dual relationships, except inasmuch as they somehow lead to violations of patient privacy rights or breaches of PHI. Professional organizations address ethical issues in social media, and for therapists, social media in professional practice is more heavily related to issues of professional ethics than HIPAA.

Therapists must be aware that social media is very public, and using or disclosing PHI in social media contexts easily can become a confidentiality breach and within the purview of HIPAA. Even non-public portions of social media are still owned by and viewable by the company that provides the social media service. Revealing PHI in any such context is almost certain to be HIPAA-noncompliant. In addition, therapists should be very careful about interacting with patients on social media, even if the relationship is not publicly acknowledged. While ethical issues are likely the main concern in such situations, it is very possible to accidentally disclose or misuse confidential information that the therapist has about a patient.

Websites: Most therapists' websites are nothing more than a brochure on the Web, in which case HIPAA has no special recommendations or requirements. Websites are a great place to post resources and self-help materials for the general patient population. Patients who visit a therapist's website do so on their own accord. Blank practice forms that do not contain PHI can be posted on therapists' websites. Allowing

patients to obtain forms by downloading them from their therapist's website is a way to avoid more risky delivery methods, such as unsecured email. (Therapists who email their patients basic practice forms most likely have not yet addressed informed consent for risks associated with unsecured email.) One issue that should be addressed in a risk analysis is how to safeguard against patients modifying digital copies of intake forms (e.g., patients removing or changing undesired pieces of information from the therapist's informed consent form without therapist's knowledge).

For therapists' websites that have more than simple brochure-like pages, a risk analysis should be done for features such as a "Contact Me" page. Most "Contact Me" pages use a website-hosting service as a carrier for the message from the visitor to the therapist. If a patient used the "Contact Me" page to send a therapist any information, the website-hosting service would be considered a Business Associate. It would be extremely unlikely that a website-hosting service would be willing to execute a HIPAA-compliant Business Associate Agreement with any of its customers. Therefore, therapists could choose to eliminate the "Contact Me" page from their website or utilize secure messaging/encrypted email services or practice management systems (PMS) that offer secure "Contact Me" pages that can link from the website or even safely embed within the website. Usually, these secure "Contact Me" pages look the same as the other webpages, and visitors may not know the difference.

Blogging: Blogging is perfectly acceptable for therapists under HIPAA. However, therapists who choose to blog must be careful about interacting with patients and should not misuse or disclose confidential information in their blogs. Patients may register on therapists' blogs and may even contribute comments. While this situation presents ethical challenges, HIPAA would regard this situation as an autonomous act on the patients' part and their own privacy decision. Regardless, therapists must not use blogging as a means for communicating PHI with patients.

Video-Telehealth and Video-Conferencing: As video-telehealth and video-conferencing are becoming increasingly common, therapists must make sure that they keep themselves updated on the storage of confidential information on computers, laptops, smartphones, tablets, and other electronic devices, as well as in the Cloud. Doxy.me, VidHealth, and VSee Clinic are free HIPAA-secure online teletherapy software platforms that provide a Business Associate Agreement to solo and small mental health practices; larger practices can access a paid version with more features. The teletherapist should begin each session with an assessment of the patient's physical location, the volume of the audio, and the proximity of other people who may overhear confidential information.

Some resources for performing risk analysis related to telehealth and video-conferencing include HIPAA COW, National Association of Social Workers (NASW) HIPAA Toolkit (available to NASW members), and Tame Your Practice. No matter what

therapists do to make their security better, they will not be HIPAA-compliant until they have completed and documented the risk analysis and risk management plan and then developed the manual of policies and procedures. No software purchase or change to computer settings can replace this process.

What considerations should be made for apps and digital assessments?

Apps: Thousands of mental health and wellness apps are often utilized as an adjunct to treatment for patients to record their symptoms and develop healthier habits. There are several key privacy concerns related to apps. Most notably, app companies can monitor data (e.g., behaviors, usernames and passwords, contact information, age, gender, phone number) and sell them to third parties. Therapists should discuss with their patients the potential threats to their PHI, the importance of remotely deleting and deactivating their digital devices in the event of loss or theft, and the risks versus benefits of using the apps in treatment.

Digital assessments: Digital assessments are becoming an increasingly popular alternative to traditional paper and pencil assessments; however, therapists must consider the risks to patient confidentiality. Therapists should discuss with patients the risks and benefits of digital assessments and offer paper-based versions if possible and preferred. iPads and other electronic devices that are used for digital assessments should be designated as such and are recommended to be used for that sole purpose to reduce risk of data breach or loss.

What safeguards should be in place for electronic medical records (EMRs)?

Electronic medical records (EMRs) are computer databases that contain patient healthcare information. They are an extremely popular and efficient way of allowing for access among healthcare providers and administrators. However, therapists should discuss with patients the risks and privacy issues related to EMRs, and therapists should be thoughtful about the level of detail included in session notes that can be accessed by other healthcare providers within the system. Potential breaches, crashes, loss of data, and storage concerns also should be addressed.

What considerations should be made for Cloud-based storage?

Cloud-based storage has gained increased popularity among therapists who wish to access files across devices and reduce the risks of natural disasters and theft/loss associated with hard copies and paper records. In addition, breach security is another reason many therapists are moving toward Cloud services in their practices. When information is kept on Cloud services, therapists can easily determine when and by whom information is accessed and to shut out people from those services when a security incident is discovered.

When possible, therapists should use "two-factor authentication" for Cloud services to safeguard against unauthorized users. They also should periodically conduct audit log reviews to check for suspicious login times and locations.

Some of the top HIPAA-compliant Cloud-based storage companies include Dropbox, Google Drive, and Microsoft OneDrive. Covered Entities who use Cloud-based storage must sign a Business Associate Agreement with the HIPAA-compliant company and also must maintain responsibility for their own electronic devices.

What is Risk Management?

Therapists are required to engage in **risk management**, a process of balancing risks and costs in an effort to reduce risks to a *reasonable* level. Risk management is not about eliminating risks entirely (which is impossible) but about reducing risks "to a reasonable and appropriate level."

Therapists will need to address the administrative, physical, and technical safeguards as part of a risk management plan. **Administrative safeguards** have to do with workforce management, training, and organizational behaviors that are essential to good security (e.g., a security incident plan, policies for vetting workforce members). **Physical safeguards** involve the physical protection of computers, vital office spaces, and equipment from intrusion, theft, natural and environmental disasters, and other threats and hazards. Finally, **technical safeguards** relate to computer access control through usernames and passwords, protection of data from confidentiality breaches, an audit trail of who accessed or altered data, etc.

What are the standards for Administrative Safeguards?

Administrative safeguards, as defined by the HIPAA Security Rule, are "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

The first Administrative Safeguard standard is the **Security Management Process, Section 164.308(a)(1),** which requires Covered Entities to "implement policies and procedures to prevent, detect, contain and correct security violations." To address Administrative Safeguards, Covered Entities must engage in **Risk Analysis** and **Risk Management**. In addition, they must implement a **Sanction Policy** "against workforce members who fail to comply with the security policies and procedures of the covered entity." Finally, Covered Entities must include an **Information System Activity Review** to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

The second Administrative Safeguard standard is **Assigned Security Responsibility, Section 164.308(a)(2),** which requires Covered Entities to "identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity." The Security Official may or may not be the same person as the Privacy Official.

The third Administrative Safeguard standard is **Workforce Security, Section 164.308(a)(3),** which requires Covered Entities to "implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information … and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information." To address Workforce Security, Covered Entities must have a **Workforce Clearance Procedure** to "determine that the access of a workforce member to electronic protected health information is appropriate." In addition, Covered Entities must implement **Termination Procedures** for "terminating access to electronic protected health information" when a workforce member leaves an organization voluntarily or involuntarily.

The fourth Administrative Safeguard standard is **Information Management, Section 164.308(a)(4),** which requires Covered Entities to "implement policies and procedures for authorizing access to electronic protected health information." To address Information Management, Covered Entities must isolate healthcare clearinghouse functions if the clearinghouse is part of a larger organization, determine whether a particular user or computer system is authorized to access PHI based on job function, and modify access as necessary.

Finally, the Administrate Safeguard requires **Security Awareness and Training, Section 164.308(a)(5),** that consists of security reminders, protection from malicious software, log-in monitoring, and password management. Covered Entities must also have **Security Incident Procedures, Section 164.308(a)(6),** to address security incidents, defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Covered Entities must also have a **Contingency Plan, Section 164.308(a)(7),** to recover ePHI in the event of an emergency or other operational disruption, such as a power outage. The Contingency Plan requires a **Data Backup plan, Testing and Revision procedures, and Applications and Data Criticality Analysis** (a prioritized list of software applications and data to determine which get restored first and which are needed at all times).

Furthermore, Covered Entities must include an **Evaluation Procedure, Section**

164.308(a)(8), to review and maintain security measures and **Business Associate Contracts and Other Arrangements, Section 164.308(b)(1),** which enable Covered Entities to permit a business associate to "create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances … that the business associate will appropriately safeguard the information." Business Associate Agreements will be discussed in greater detail in the HIPAA Omnibus Final Rule section.

For further information on Administrative Safeguards, click on the following link to the Department of Health and Human Services: Administrative Safeguards.

What are the standards for Physical Safeguards?

The HIPAA Security Rule defines **Physical Safeguards** as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

The first Physical Safeguard standard involves **Facility Access Control, Section 164.301(a)(1),** which requires Covered Entities to "implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed." To address Facility Access Control, Covered Entities must implement **Contingency Operations** procedures that "allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency." Covered Entities also must have a **Facility Security Plan** (e.g., locked doors, alarms, surveillance cameras, visitor badges, property control tags or engraving on equipment) that secures the facility from theft, tampering, and unauthorized access. Covered Entities also are required to have **Access Control and Validation Procedures** to "control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision." **Maintenance Records** are required to document repairs and changes to the facility that are related to security.

The second Physical Safeguard standard involves **Workstation Use, Section 164.310(b),** which requires Covered Entities to "implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information." Workstations are defined as any electronic device, such as a laptop or desktop computer, that accesses and/or stores electronic data.

The third Physical Safeguard standard is **Workstation Security, Section 164.310(c),** which requires Covered Entities to "implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."

Covered entities are required to use **Device and Media Controls, Section 164.310(d)(1),** that "govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within a facility." Covered entities should have policies related to disposal, media re-use, accountability, and data backup and storage.

For further information on Physical Safeguards, click on the following link to the Department of Health and Human Services: Physical Safeguards.

What are the standards for Technical Safeguards?

HIPAA Security Rule defines **Technical Safeguards** as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

The first standard related to Technical Safeguards is **Access Control, Section 164.312(a)(1),** which requires Covered Entities to "implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." To address Access Control, Covered Entities should have **Unique User Identification** to track specific users' activity. Using an employee name or variation of the name is easier for authorized users and management to recognize, but random numbers and characters are more difficult for unauthorized users and hackers to guess. Covered entities also must have an **Emergency Access Procedure** that is established and implemented for obtaining ePHI in emergencies. Covered Entities also should have **Automatic Logoff** procedures that prevent unauthorized users from accessing ePHI if someone leaves a workstation unattended for a certain period of time. Finally, Covered Entities should have **Encryption and Decryption** procedures to convert text to encoded data based on an algorithm and safeguard against unauthorized users who do not have the key to convert the encrypted data back into text.

Audit Controls, Section 164.312(b), is the second standard related to Technical Safeguards. Covered Entities must "implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." These measures are especially important in determining if there has been a security violation.

The third standard related to Technical Safeguards is **Integrity, Section 164.312(c)(1),** the process of determining that "data or information have not been altered or destroyed in an unauthorized manner." Covered Entities must have a **Mechanism to Authenticate Electronic Protected Health Information** (e.g., digital signatures or other means to protect integrity of ePHI).

Fourth, Covered Entities must utilize **Person or Entity Authentication, Section 164.312(d)** "to verify that a person or entity seeking access to electronic protected health information is the one claimed." For example, a Covered Entity may require a password, PIN, smart card, key, fingerprint, or facial recognition system to prove identity.

Transmission Security, Section 164.312(e)(1), is the final standard related to Technical Security. Covered Entities must "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communication network." To address Transmission Security, Covered Entities may use **Integrity Controls** and **Encryption** (as discussed previously).

For further information on Technical Safeguards, click on the following link to the Department of Health and Human Services: Technical Safeguards.

Table 3: Five Security Components for Risk Management[2]

Security Component	Examples of Vulnerabilities	Examples of Security Mitigation Strategies
Administrative Safeguards	• No security officer is designated. • Workforce is not trained or is unaware of privacy and security issues. • Periodic security assessment and	• Security officer is designated and publicized. • Workforce training begins at hire and is conducted on a regular and frequent basis. • Security risk analysis is performed periodically and when a change occurs in the practice or the technology.
Physical Safeguards	• Facility has insufficient locks and other barriers to patient data access. • Computer equipment is easily accessible by the public. • Portable devices are not tracked or not locked up when not in use.	• Building alarm systems are installed. • Offices are locked. • Screens are shielded from secondary viewers.
Technical Safeguards	• Poor controls allow inappropriate access to EHR. • Audit logs are not used enough to monitor users and other EHR activities. • No measures are in place to keep electronic patient data from improper changes. • No contingency plan exists. • Electronic exchanges of patient information are not encrypted or otherwise secured.	• Secure user IDs, passwords, and appropriate role-based access are used. • Routine audits of access and changes to EHR are conducted. • Anti-hacking and anti-malware software is installed. • Contingency plans and data backup plans are in place. • Data is encrypted.
Organizational Standards	• No breach notification and associated policies exist. • Business Associate (BA) agreements have not been updated in several years.	• Regular reviews of agreements are conducted and updates made accordingly.
Policies and Procedures	• Generic written policies and procedures to ensure HIPAA security compliance were purchased but not followed. • The manager performs ad hoc security measures.	• Written policies and procedures are implemented and staff is trained. • Security team conducts monthly review of user activities. • Routine updates are made to document security measures.

What is a Cost-Benefit Analysis?

When therapists consider which security measures to put into place in their practice, they need to do a cost-benefit analysis for each measure to determine if it is right for

[2] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

their practice. The cost-benefit analysis must consider each of the following four factors:

- size, complexity, and capabilities of the covered entity (e.g., a solo practitioner without IT support has far less complexity and capability than a large clinic or hospital with an IT department),
- the covered entity's technical infrastructure, hardware, and software security capabilities (e.g., a solo practitioner typically has the same equipment as the average person and does not have IT expertise),
- costs of security measures (e.g., some affordable options are encryption of computers, tablets, and smartphones; a secure e-mail service, such as Hushmail; HIPAA-secure video-conferencing options, such as VSee and Doxy.me, instead of Skype, which is free but not HIPAA-secure; HIPAA-compliant billing platforms), and
- probability and criticality of potential risks to ePHI (e.g., examining whether certain risks are worth taking if appropriate security measures are too expensive or difficult to implement)

In the event that therapists decide that a risk ranks somewhat low and that adding a new security measure seems like a wasteful expense, they may decide to accept the risk, which is an acceptable practice in security risk management and in compliance with HIPAA. Therapists would need to document their reasoning when accepting a risk and explain how the risk is low enough to be left alone.

Low-Cost, Highly Effective Safeguards

- Say "no" to staff requests to take home laptops containing unencrypted ePHI.
- Remove hard drives from old computers before you get rid of them.
- Do not email ePHI unless you know the data is encrypted.
- Make sure your server is in a room accessible only to authorized staff, and keep the door locked.
- Make sure the entire office understands that passwords should not be shared or easy to guess.
- Notify your office staff that you are required to monitor their access randomly.
- Maintain a working fire extinguisher in case of fire.
- Check your EHR server often for viruses and malware.

https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

What Is a Security Policies and Procedures Manual?

Finally, therapists are required to have a **Security Policies and Procedures Manual** that is informed by their risk management planning decisions and is for therapists and

anyone else who assists in their practice (not for patients). Quite a few of therapists' risk management decisions will involve some kind of policy or procedure, such as a plan for how to do computer backups (i.e., method of backup, schedule, and plan for confirming the backups are working) and how to train new people in the practice for maintaining patient confidentiality. The manual needs to address all the risk management measures described in the three areas of the Security Rule (i.e., Administrative, Physical, and Technical) as well as any other policies and procedures they determine that they need to address from the risk analysis.

The following link to the Department of Health and Human Services provides a useful guide to risk analysis and risk management: Basics of Risk Analysis and Risk Management

Section V
Breach Notification

HIPAA's Final Breach Notification Rule states that, when therapists suffer a data breach involving unsecured (e.g., unencrypted) PHI, they must notify all impacted patients and the Office for Civil Rights (OCR) about the breach. Generally, breaches involve the confidentiality of information; however, some states and licensing boards also may require therapists to notify them of breaches to the availability or integrity of records (e.g., lost or prematurely destroyed records).

Table 4: Comparison of Secured and Unsecured PHI[3]

Secured PHI	Unsecured PHI
An unauthorized person cannot use, read, or decipher any PHI that he/she obtains because your practice: • Encrypts the information; or • Clears, purges, or destroys media (e.g., data storage devices, film, laptops) that stored or recorded PHI; • Shreds or otherwise destroys paper PHI. (These operations must meet applicable federal standards.[128])	An unauthorized person may use, read, and decipher PHI that he/she obtains because your practice: • Does not encrypt or destroy the PHI; or • Encrypts PHI, but the decryption key has also been breached.

What is a Privacy Officer?

All practices, but especially small ones, should consider which consequence are likely to befall them in a typical data breach and should delegate a **Privacy Officer** (in solo practices, often the practitioners themselves). The Privacy Officer is responsible for the development of the initial and ongoing implementation of HIPAA-related privacy practices as well as other policies and procedures in the psychotherapy practice. The Privacy Officer maintains responsibility for handling requests for or accounts of disclosures of records, periodically reviews privacy policies sand other HIPAA regulations, keeps up with changes in regulations and implements any necessary changes to forms and policies, trains staff and responds to their questions, and addresses complaints and corrective actions, if necessary. A simple announcement in a visible location in the practice should include the following: "Our Privacy Officer is XXXXX. The Privacy Officer can: (a) answer your questions about our privacy practices;

[3] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

(b) accept any complaints you have about our privacy practices; and (c) give you information on how to file a complaint. You can contact the Privacy Officer by calling XXXXX."

How are breaches assessed?

Breaches begin as "**security incidents**," such as a missing computer that holds patient information, a patient record file left on a desk in an unlocked room, or a stolen smartphone that contains patients' texts and emails. When therapists discover a security incident, HIPAA allows therapists 60 days to work to mitigate the impact of the breach, assess the outcome, and determine if an actual breach occurred. However, most states require a shorter period of time, so preemptive analysis is necessary.

What are a Security Incident Response Procedure and Four-Point Assessment?

As part of the Security Rule, therapists should have formulated a **Security Incident Response Procedure,** a written plan on how they will respond to security incidents, including contacting an attorney. Therapists must work to mitigate the breach in various ways, such as utilizing their smartphone tracking service to remotely delete their phone before thieves can access its data.

Next, therapists must run a **four-point assessment** of security incidents before making a breach notification:

1. the nature of the breached information and what kind of PHI was breached (e.g., Social Security numbers, diagnoses, patient initials),
2. the party or parties to whom the information was breached (e.g., a healthcare colleague who knows how to ethically handle the situation versus someone whose intent was malicious or unknown),
3. whether there is a chance for the breached PHI to be retained (e.g., assessing whether someone *could* access PHI versus actually *did* access the material), and
4. how the breach was handled (e.g., therapists immediately contacted the unintended recipient of a confidential fax and had the documents shredded before reading).

Based on the four-point assessment, if the covered entity determines that there was not a significant risk that PHI was compromised, a breach notification is not required.

The Breach Notification Rule shifted the **burden of proof** from the Office for Civil Rights to the Covered Entity or Business Associate. Prior to the Breach Notification Rule, the Office for Civil Rights had to prove that harm had occurred due to HIPAA-noncompliance. With the Breach Notification Rule, the burden of proof rests on the Covered Entity or Business Associate to prove that the breach did *not* happen if they

are not reporting a breach. They must write up an assessment and retain it in their HIPAA records. Consulting with a relevant security expert and an attorney are strongly advised.

What are different breach levels, and how must Covered Entities report these breaches?

HIPAA defines two levels of breach: (1) small breaches (i.e., below 500 affected individuals), and (2) large breaches (i.e., 500 or more affected individuals).

For small breaches, the Covered Entity has until the end of the year to notify the Office for Civil Rights. However, as soon as possible, therapists must send breach notification letters via first class mail to patients whose unsecured PHI was accessed, stolen, or lost. The letter should be sent to the patients' last known address and include in plain language an explanation of the nature of the breach, what information was exposed or stolen, what the therapist is doing in response to the breach to minimize harm, what actions the patients can take to minimize harm, and what the therapist will do to prevent future breaches. If current mailing information is not known for 10 or more affected individuals, the Covered Entity must upload a breach notice to his or her website and link it from the home page for 90 days in a prominent location. Other means of contacting affected individuals, such as notification via telephone, should be used as well.

For large breaches, the Covered Entity must send an electronic notification to the Office for Civil Rights immediately, run ads in the local media to notify the public of the breach and help ensure that all breach victims are informed of the potential PHI exposure, and set up identity theft and credit monitoring services for the affected patients. The media ads and notifications sent to affected patients must advertise that these theft and credit monitoring services are available and explain how to enroll in them. Therapists also must consider state laws and licensing board requirements related to breach notifications.

What information does the Office for Civil Rights need for a breach notification?

Breach notifications must be sent to the Office for Civil Rights by using the following link: File a Breach: General Tab (hhs.gov). The Covered Entity will be required to provide the following information within this electronic form:

- Covered Entity's contact information,
- start and end dates of the breach,
- start and end dates of the breach discovery,
- approximate number of individuals affected by the breach,

- type of breach (i.e., hacking/IT incident, improper disposal, loss, theft, unauthorized access/disclosure),
- the location of the breach (i.e., desktop computer, electronic medical record, email, laptop, network server, other portable electronic device, paper/films),
- type of PHI involved in the breach (i.e., clinical, demographic, financial),
- safeguards in place prior to the breach (i.e., Privacy Rule Safeguards, Security Rule Administrative, Physical, and Technical Safeguards),
- how and when affected individuals and the media were notified,
- actions taken in response to the breach (e.g., changed/strengthened password, new safeguards and security, staff training, sanctioned workforce members), and
- a signed attestation that the above information is accurate and complete.

What is a Safe Harbor?

The Final Breach Notification contains a **safe harbor** that immunizes Covered Entities from the rule when they can demonstrate that the stolen or missing data are well secured. If the data are "at rest" and are fully encrypted and in a locked state, then they can meet the safe harbor standard. However, the standard for data in motion (i.e., being transmitted) is not quite as straightforward and requires examination of the software used. Therapists must consult with their software providers.

Covered Entities must stay abreast of breach policies, and therapists who do not comply with HIPAA rules are subject to monetary and criminal penalties. States have their own breach notification laws, typically requiring prompt notification of breach victims and notices submitted to the state attorney general's office in shorter timeframes than HIPAA requires for Office for Civil Rights notification. Therefore, Covered Entities must remain informed about state laws that preempt HIPAA. [See "Breach Assessment" form at the end of the Kit.]

Section VI
HIPAA Transaction and Omnibus Rules

In 2009, HIPAA updated its Transaction Rules related to **Electronic Data Interchange (EDI),** the exchange of electronic data from one computer to another. HIPAA requires all insurance companies and therapists to use standardized forms for all electronic claims or other covered transactions. For mental health, the X12 837 or ANSI 837 Professional Form replaces the old HCFA 1500 claims form. While HIPAA does not mandate the use of electronic claims, the purpose of the uniformity in electronic transactions is to streamline efficiency in claims and reduce costs. Note that HIPAA also does not mandate the use of clearinghouses which act as intermediaries between therapists and insurance companies by translating therapists' bills into electronic bills that are acceptable to insurance companies. Insurance companies who process insurance claims electronically are only required to accept The *International Classification of Diseases* (ICD-10-CM) diagnosis codes; therefore, therapists need to convert their *Diagnostic and Statistical Manual of Mental Disorders* (DSM-5) diagnosis codes into their ICD-10-CM equivalents.)

What is a National Provider Identifier (NPI)?

A **National Provider Identifier (NPI)** is a 10-position numeric identifier akin to a Social Security number (SSN) or Employee Identification Number. NPIs are issued by the National Provider System (NPS), an agency in the Center for Medicare and Medicaid Services (CMS). Once a therapist is assigned a number, it will stay with him or her until retirement or death. NPIs contain no "embedded intelligence," meaning that it contains no information about the provider, such as state, gender, or even profession.

Any therapist who deals with insurance companies, whether electronically or not, are likely to benefit from having an NPI. Therapists in private practice should get their own NPI, while practitioners employed by clinics, agencies, and counseling corporations will use the NPI that the organization has assigned. While Covered Entities must obtain an NPI, therapists who are not considered Covered Entities may also obtain it. Obtaining an NPI does not turn a therapist who is not considered a Covered Entity into one who is considered a Covered Entity.

The HIPAA Omnibus Final Rule (2013)

The HIPAA Omnibus Final Rule (2013) made several final additions to the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule. A few are highlighted below:

What is a Business Associate, and What is a Conduit Exception?

The HIPAA Omnibus Final Rule made some changes to the definition of a Business Associate in an effort to clarify and expand what entities are obligated to comply with HIPAA regulations. Generally, if a service keeps or views any of the transmitted data, it is considered a Business Associate. Janitorial services, plumbers, electricians, photocopy machine repairment, and others who provide services *within* the therapists' office are not considered Business Associates.

Services may be exempted from the Business Associate rule if they qualify as a **conduit** (i.e., a service that simply moves PHI from one place to another). For companies to qualify as conduits, they must never persistently store any PHI and must not be able to view the PHI they are transmitting. Services that are considered conduits and therefore are exempted from the Business Associate rule include delivery truck line employees, the United States Postal Service, and the United Parcel Service. In the case of ePHI, the data must be encrypted, and the conduit must not have access to the encryption key.

Per the Omnibus Final Rule, Skype and Facetime are specifically considered to be Business Associates. Many therapists wish to use Skype and Facetime because they are free; however, both Skype and Facetime miss the mark for healthcare security and should not be used for communication with patients per HIPAA guidelines. In addition, it is very unlikely that any telemental health software would qualify as a conduit. Therefore, therapists should not use any software service for telemental health without a Business Associate Agreement.

Financial institutions also are given a very narrow exemption from the Business Associate rule. Basic transactions that are necessary for getting paid are exempt from HIPAA (e.g., depositing a check, running a payment card, transferring funds, making electronic payments through services such as PayPal or Google Wallet). However, modern financial organizations that provide services above and beyond simple payment processing are considered Business Associates. These include invoicing services, accounting services where the data includes PHI, and debt collection services. Before the HITECH Act of 2009, Business Associates had a "contractual obligation" with Covered Entities to be HIPAA-compliant but there was no HIPAA enforcement of Business Associates for violations. Covered Entities also could claim ignorance about whether the Business Associate was HIPAA-noncompliant. Since the HITECH Act,

Business Associates are required to sign a Business Associate Agreement with the Covered Entity, are held to the same legal standard to protect PHI as the Covered Entity, and are must report data breaches to the Covered Entity. The Omnibus Final Rule extends the HITECH Act requirements to make Business Associates subject to HIPAA audits and civil and criminal penalties, just as Covered Entities.

What is a Business Associate Agreement?

HIPAA mandates that therapists establish with Business Associates a **Business Associate Agreement.** A Business Associate Agreement requires these organizations or people to maintain HIPAA compliance when handling PHI or electronic PHI (ePHI). The Business Associate Agreement must specify what PHI is provided to the Business Associate and many other important responsibilities of the Business Associate, with the following three highlighted here: (1) it will not violate the contract related to use and disclosure of PHI; (2) it will utilize appropriate safeguards to prevent unauthorized disclosures; and (3) will report any use, disclosure, or breaches. Although must most Business Associates have contracts ready, therapists must verify that documents are HIPAA-compliant. If a therapist fails to obtain "satisfactory assurances" that a Business Associate is HIPAA-compliant before utilizing its services, the therapist can be considered liable for a breach of unsecured PHI.

Once the HIPAA-compliant Business Associate Agreement is executed, the document indemnifies the therapist from liabilities that arise if the Business Associate suffers a data breach that impacts the therapist's information. However, therapists still must inform their patients when their confidentiality has been breached by a third party and should terminate contracts with Business Associates that are negligent. Unless there is a specified termination date, the Business Associate Agreement remains valid indefinitely; however, these agreements should be reviewed at least once per year so that the Covered Entity may obtain the Business Associate's most recent risk assessment and check that there are no changes in state or federal laws that must be considered.

It is important to note that the Business Associate Agreement is a legal and professional responsibility and is entirely between the Covered Entity and the Business Associate; the Business Associate Agreement is not a patient right, and patient consent cannot impact the legal need for it.
The following is a sample Business Associate Agreement that is provided in Form II and is directly copied from the Department of Health and Human Services website (Business Associate Contracts | HHS.gov):

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and

the permitted uses and disclosures by the business associate of the de-identified information.]
(b) Business associate may use or disclose protected health information as required by law.
(c) Business associate agrees to make uses and disclosures and requests for protected health information
[Option 1] consistent with covered entity's minimum necessary policies and procedures.
[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]
(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]
(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.
(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.
(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.
(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.
(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or

is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;

2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

What are some considerations around marketing based on the HIPAA Omnibus Final Rule?

The Omnibus Final Rule also expands the uses and disclosures of protective health information (PHI) that are considered **marketing.** Marketing includes communications about health-related products or services if the Covered Entity receives "financial remuneration" in exchange for marketing the communication from or behalf of the third party whose product or service is being described. Financial remuneration is

defined as payments in exchange for making marketing communications. It does not include non-financial benefits, refill reminders or other communications about a drug currently prescribed to an individual, telephone communications for marketing, communications promoting general health that do not promote a product or service from a particular provider, or communications about government-sponsored programs. Many of these changes are not applied to non-psychiatrists, psychotherapists, and mental health practitioners in solo private practice.

What are some considerations around emails and texts?

HIPAA Omnibus Final Rule also states that Covered Entities are permitted to send patients **unencrypted emails and texts** containing confidential information, only if two conditions are met: (1) the patient requests to receive unencrypted digital communication, and (2) the patient has been advised of the risks of sending PHI by unsecured email or text message. The 2013 Omnibus Rule clarification on this issue is indicative of HIPAA's rigorous support of patients' right of autonomy and informed consent regarding risks associated with unencrypted communication.

Simply because patients are permitted to accept the risks of unsecured emails and texts under HIPAA does not always mean that therapists and patients should do so. Both parties need to be aware of what kinds of Internet communications are genuinely risky and how those risks impact each individual patient before proceeding. Therapists also should be aware of blurred lines between using unsecured email and texting for administrative issues and performing telemental health services by unsecured email or text. Telemental health experts urge therapists to obtain special training in telemental health services, and some licensing boards restrict or even ban email/text-based telemental health services. Professional ethics codes (e.g., 2014 American Counseling Association Code of Ethics) and state laws may have higher standards than HIPAA and preempt HIPAA. [See "Authorization to Use Unencrypted Email and Text" form at the end of the Kit.]

Encrypted email is generally a very secure way to send sensitive information to patients and is a reliable part of a risk management plan. Like all Cloud services, HIPAA requires a Business Associate Agreement with secure messaging/encrypted email service providers. Many online practice management systems (PMS) include "client portals" that allow for secure messaging.

Setting up two-factor authentication for emails is an additional safety step. Two-factor authentication involves a login password followed by a text message to a registered device that contains a code that the therapist then types into the computer. Even if a hacker accesses a therapist's password, the hacker cannot retrieve the email because he or she cannot complete the second step of the authentication process.

In addition, there are many issues to consider related to texting. Texting may refer to many services, including apps that allow individuals to text without phone service (e.g., WhatsApp, Snapchat, Viber, Signal, Wickr). In these cases, a Business Associate Agreement is necessary unless the service provider meets the conditions as a conduit. Note that VoIP internet services require Business Associate Agreements, while text messaging services through classic phone companies do not require Business Associate Agreements at the time of this writing. Just because a Cloud texting service uses "end-to-end encryption" for messaging does not guarantee that the service does not retain information about text messages with patients. Therapists also must bear in mind that, if an app deletes text messages from patients before the messages can be retained, therapists have lost records that they are legally required to keep.

What are some consequences for HIPAA noncompliance per the Omnibus Rule?

Finally, the Final Omnibus Rule introduces a new four-level penalty tier system for monetary fines based on the level of culpability related to HIPAA noncompliance. Adjusted for inflation, as of this writing, Tier 1 (Reasonable Efforts) has a minimum penalty of $127 and maximum penalty of $63,973 per violation. Tier 2 (Lack of Oversight) has a minimum penalty of $1,280 and a maximum penalty of $63,973 per violation. Tier 3 (Neglect – Corrected) has a minimum penalty of $12,794 and a maximum penalty of $63,973 per violation. Tier 4 (Neglect – Not Corrected Within 30 Days) has a minimum penalty of $63,973 and a maximum penalty of $1,919,173 for violation. All tiers have an annual penalty limit of $1,919,173. In 2011, the Office for Civil Rights also began conducting compliance audits, which demonstrated that many Covered Entities were noncompliant and which have resulted in serious multimillion-dollar financial penalties in some cases.

Starting in 2009, The HITECH Act directed the Office for Civil Rights to publish a breach portal (nicknamed the "HIPAA Wall of Shame") on its website. The breach summaries include the name of the Covered Entity or Business Associate, the type and location of the breach, and the number of affected individuals.

For a helpful HIPAA guide from the Office of the National Coordinator for Health Information Technology that includes recommendations through the Omnibus Final Rule, click on the following link: Guide to Privacy and Security of Electronic Health Information (healthit.gov)

Section VII
HIPAA Updates Since the Omnibus Final Rule

How did the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 align regulations more closely with HIPAA?

The goals of the CARES Act of 2020 were to ensure that every American had access to necessary healthcare and to take measures against the economic consequences of the coronavirus pandemic. The CARES Act expanded healthcare providers' rights to share PHI for patients with substance abuse disorders, simultaneously making stricter requirements in the event of a confidentiality breach. The CARES Act allows patients with substance abuse disorders to grant broad consent for their records to be shared by a Covered Entity or Business Associate for any reason related to treatment, payment, or healthcare operations (TPO). Uses and disclosures of PHI are limited to the minimum necessary information, and patients may withdraw their consent in writing at any time. These changes are more closely aligned with HIPAA.

What temporary Notification of Enforcement Discretion allowances were issued during the COVID-emergency?

In 2020, the Office for Civil Rights issued guidance for telehealth during the COVID-19 public health emergency. The U.S. Department of Health temporarily (1) permitted HIPAA-enforcement discretion for **"good faith" treatments** that utilized remote communication tools normally not considered HIPAA-compliant and (2) did not require that Covered Entities enter into Business Associate Agreements with providers of remote communication tools.

According to the Office for Civil Rights' FAQs on Telehealth and HIPAA, examples of **"bad faith" treatments** that would *not* be covered under enforcement discretion allowance include the following:

- criminal acts (e.g., fraud, identity theft, intentional invasion of privacy), prohibited disclosures of patient data during a telehealth communication (e.g., sale of data),
- "violations of state licensing laws or professional ethical standards that result in disciplinary actions related to the treatment offered or provided via telehealth," and
- unacceptable means of public-facing remote communication products (e.g., TikTok, Facebook Live, Twitch, public chat rooms). Public-facing products are

not permitted because they are "designed to be open to the public or allow wide or indiscriminate access to the communication."

Covered Entities must be prepared to adhere their telehealth services to HIPAA standards once the Department of Health and Human Services declares an end to the COVID-19 public health emergency. Financial penalties can arise for HIPAA violations after the COVID-19 public health emergency is ended and the period of enforcement discretion expires.

What is the HIPAA Safe Harbor Law (2021)?

In 2021, President Donald Trump signed the HIPAA Safe Harbor Bill (HR 7898) into law and updated President Obama's HITECH Act. The 2021 Safe Harbor Law requires the U.S. Department of Health and Human Services to consider the best practices related to cybersecurity that the Covered Entity utilized in the 12 months prior to any data breach when evaluating punitive actions and financial penalties from security breaches.

What HIPAA updates are expected in late 2022 or soon thereafter?

Although there have been few major changes to HIPAA rules since 2013, changes related to the Privacy Rule are expected in late 2022 or soon thereafter. The process for making changes to HIPAA is slow as the Department of Health and Human Services solicits feedback on regulations that are problematic or obsolete. Next, the Department issues a **Notice of Proposed Rulemaking (NPRM),** followed by period of comments from members of the healthcare industry. Only then is a final revision issued, with a grace period for compliance with the new regulations. Typical grace periods for compliance with the new rules are one or two years.

The Department of Health and Human Services published a Notice for Proposed Rulemaking for proposed changes to the HIPAA Privacy Rule on January 21, 2021. Although the Privacy Rule traditionally has focused on restricting uses and disclosures of PHI, the expected changes allow for more freedom in healthcare information flow and improved patient access rights. Among some of the proposed HIPAA regulations are allowing patients to photograph their PHI and reducing the maximum time for therapists to provide patients with requested PHI from 30 days to 15 days. Many of the proposed changes would pose challenges to healthcare workers, so the period of comments for healthcare industry stakeholders provides an opportunity for discussion and compromise. For example, allowing patients to photograph their PHI would require that Covered Entities develop procedures for ensuring that patients do not photograph PHI that they are not authorized to view. Similarly, healthcare workers may have difficulty providing patients with access to PHI in a shorter time period because billing records are often stored in a separate system from other healthcare information, yet both constitute their Electronic Health Record (EHR). Based on commentary from

the healthcare industry, several proposed regulations from the Notice for Proposed Rulemaking may not be adopted into law.

As always, the HIPAA link directly from the U.S. Department of Health and Human Services provides a wealth of information for therapists to keep abreast of updates: HIPAA Home | HHS.gov.

Section VIII
HIPAA and Its Relationship with State Laws and Professional Guidelines

What is a preemption analysis?

Throughout the Kit, there has been an emphasis on **preemption analysis,** the voluminous and complex task of comparing, line by line, HIPAA and state and professional regulations in order to determine which one preempts the others. The preemption analysis determines which rules and regulations must be followed and is the job of skilled and meticulous teams of attorneys and other experts. Therapists must be aware of the enormity of state-by-state preemption analysis.

The purpose of the Kit is to give readers some basic tools and assumes that they know the important local and state laws and regulations and their own professional association's ethics codes and consult with the proper experts. Readers may obtain the preemption analysis for their state by contacting their state HIPAA implementation office (or equivalent agency), licensing board, state professional association, or national professional association.

Under what circumstances does HIPAA preempt state laws?

The Federal Privacy Rule is designed to provide a minimum standard or national "floor" of privacy protection. HIPAA takes precedence over state laws that provide less privacy protection or less autonomy for patients and provide patients with less access to or control over their mental health records.

HIPAA preempts existing state laws in the following scenarios:

- if it is necessary to prevent fraud and abuse, addresses controlled substances,
- is needed for insurance regulations or reporting on healthcare delivery,
- is more stringent for reporting disease, injury, child abuse, birth and death, or for public health initiatives, or
- relates to audits, monitoring, licensing, or credentials.

Under what circumstances do state laws preempt HIPAA?

Therapists generally must follow whichever laws are more restrictive or provide more autonomy and privacy. Many state laws before 2003 were more stringent than HIPAA requirements related to privacy and protection of mental health records and, therefore, preempt HIPAA. For example, the Federal Privacy Rule gives Covered Entities 30 days to respond to a patient's request to inspect his or her own PHI, while California law requires a response within 5 business days. Therapists in California must follow the stricter standard; in this case, they must provide access within 5 business days. Similarly, California data breach notification law only provides therapists with 15 days to investigate data breaches, whereas HIPAA's Breach Notification Rule allows 60 days. In this case, California therapists must follow the stricter standard, California data breach notification law.

Using California state law further as an example, California law also preempts HIPAA regulations in regard to parental access to a minor's record. The federal regulations aim to avoid interfering with parental authority issues; however, California law is very explicit with regard to parental rights to minors' medical information, and therapists must generally disclose information about treatment to parents, except when the law permits a minor to consent to treatment without parental consent (i.e., when a minor is emancipated, when a minor is in a situation at risk or in a situation where requiring parental permission might discourage necessary treatment). In general, California law gives much more protection to HIV/AIDS information, compared to federal regulations that do not address HIV/AIDS information at all.

There are three exceptions where state law preempts a conflicting HIPAA regulation:

- when a state law provides for the reporting of disease or injury, child abuse, births or deaths, or for the conduct of public health surveillance, investigation, or intervention,
- when state law requires a health plan to report or to provide access to information for the purpose of management and financial audits, program monitoring and evaluation, or licensure or certification, and
- when, at the request of a State Governor, the Secretary of the Department of Health and Human Services determines that a particular provision of state law is necessary.

Covered Entities should not exercise independent judgment when dealing with the above exceptions. Instead, they should consult and use a formal process conducted by the state.

Under what circumstances do professional guidelines preempt HIPAA?

As has been mentioned many times in the Kit, ethics codes may be more stringent than HIPAA regarding the need to acquire patient consent before disclosing PHI. Therefore, ethics codes would preempt HIPAA in these cases.

The relationship between HIPAA regulations and the professional association code of ethics depends on whether the professional organization adopts HIPAA regulations in whole or in part into its code or into separate guidelines. It also depends on whether the state incorporates the professional code of ethics into its licensing laws or not. HIPAA has increasingly become the standard of care.

Indeed, major ethics codes and guidelines have incorporated HIPAA principles related to secure electronic transmissions of client information:

- The Ethical Principles of Psychologists and Code of Conduct (2016) issued by the American Psychological Association states, "Psychologists have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium, recognizing that the extent and limits of confidentiality may not be regulated by law or established by institutional rules or professional or scientific relationship" (APA Ethical Principles of Psychologists and Code of Conduct, 2016, 4.01).

- The Code of Ethics (2014) from the American Counseling Association states, "Counselors use current encryption standards within their websites and/or technology-based communications that meet applicable legal requirements. Counselors take reasonable precautions to ensure the confidentiality of information transmitted through any electronic means" (ACA Code of Ethics, 2014, H2.d).

- The Code of Ethics (2017) for the National Association of Social Workers (NASW) states, "Social workers should take reasonable steps to protect the confidentiality of electronic communications, including information provided to clients or third parties. Social workers should use applicable safeguards (such as encryption, firewalls, and passwords) when using electronic communications such as email, online posts, online chat sessions, mobile communication, and text messages" (NASW Code of Ethics, 2017, 1.07m).

- The Code of Ethics (2015) for the American Association for Marriage and Family Therapists (AAMFT) states, "Therapists and supervisors are to ensure that all documentation containing identifying or otherwise sensitive information which is electronically stored and/or transferred is done using technology that adheres to standards of best practices related to confidentiality and quality of services and that meet applicable laws. Clients and supervisees are to be made aware in

writing of the limitations and protections offered by the therapist's or supervisor's technology" (AAMFT Code of Ethics, 2015, 6.4)

- The Code of Ethics (2016) for the National Board for Certified Counselors states, "National Certified Counselors (NCCs) shall act in a professional manner by protecting against unauthorized access to confidential information. This includes data contained in electronic formats. NCCs shall inform any subordinates who have physical or electronic access to information of the importance of maintaining privacy and confidentiality" (NBCC Code of Ethics, 2016, 56).

- The Code of Ethics (2011) for the California Association of Marriage and Family Therapists (CAMFT) states, " Marriage and family therapists are aware of the possible adverse effects of technological changes with respect to the dissemination of patient information and take care when disclosing such information. Marriage and family therapists are also aware of the limitations regarding confidential transmission by Internet or electronic media and take care when transmitting or receiving such information via these mediums" (CAMFT Code of Ethics for Marriage and Family Therapists Part I, 2011, 2.3).

How should therapists consider all the information from HIPAA, state laws, and professional guidelines?

The decision-making process for a particular situation should include clinical, ethical, and legal analysis and should cover the following elements:

- client factors, such as history, economic status, culture, and language,
- context factors, such as educational, clinical outpatient, or forensic settings,
- clinical considerations, such as diagnosis, dangerousness, and personality disorders,
- ethics codes that are relevant to the case,
- HIPAA preemption analysis, and
- standard of care.

It is of utmost importance that the decision-making process and the considerations of different options are documented in detail in the clinical records.

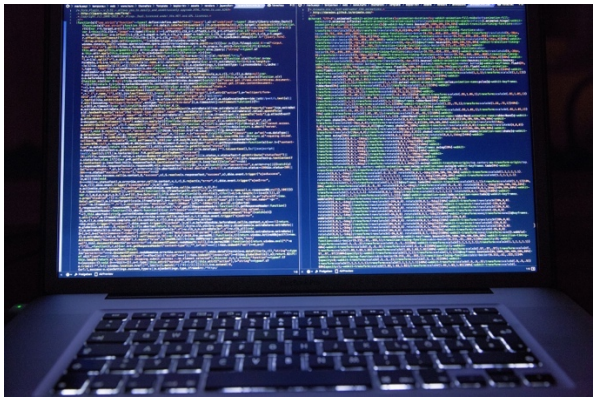
HIPAA does not police compliance with state regulations, which remains the responsibility of state authorities. Conversely, state boards do not police and regulate HIPAA laws. The notable exception is that the State Attorneys General may enforce HIPAA in their states.

If both HIPAA and state laws "permit" but do not "require" disclosure, therapists may not need to disclose at all. Therapists must do a careful analysis and seek consultation, if necessary.

Discrepancies between the professional codes of ethics are inevitable, and most codes state that the ethical rules are always subject to modification to conform to the law, whether it be state law, HIPAA law, or case law. Ethics codes of different professions differ, and there are also different laws within states for various professions.

Each practitioner must learn to navigate the complexities of his or her own profession and state, as well as ever-evolving HIPAA regulations. State laws, professional codes of ethics, and HIPAA continue to change over time.

Section IX
Risk Analysis and Security Policy & Procedure



As noted previously, it is incumbent on each organization to engage in ongoing risk analysis and security reviews. The extent and frequency will depend on the size of the organization. Many of the rules were written for larger organizations and did not have solo or small group practices in mind. Nonetheless, these requirements are written into HIPAA guidelines.

In addition to the HIPAA compliance checklist provided in form 1, the following link will take you to sections of a brochure published by the National Coordinator for Health Information Technology which can be used as guidance on maintaining compliance.

Privacy and Security Guide

HIPAA Made Friendly

Section X
Ready-to-Adapt Forms

Psychotherapists are permitted modify the forms included in the Kit to suit their own personal and professional needs. Forms as a Word document can be found here. They may simply copy and paste the forms into their computer and then insert their letterhead, name, or any other changes that apply to their setting and practice. Therapists should be sure that they comply with the legal, ethical, and clinical regulations of their profession and state as they adapt these forms for their own use.

Forms Below:

Form I:
The HIPAA Compliance Checklist

Insert your letterhead here

This form is intended to serve as a sample of a HIPAA checklist. Add to it as you see fit. This document should be placed in the HIPAA folder, as it is a very important part of your documentation of compliance.

THE HIPAA COMPLIANCE CHECKLIST

Change and adapt this checklist as appropriate and applicable to your practice, profession, and state.

Legal Name of Practice Entity:
Type of practice: Psychotherapy/Counseling/Mental Health
Address(es):
Phone:
Fax:
E-mail:

Privacy Officer: The Privacy Officer, who is designated to develop and implement privacy policies and procedures, is: _____ Privacy Officer can be reached at phone #: _____

Security Officer: The Security Officer, who is designated to develop and implement security policies and procedures, is: _____ Security Officer can be reached at phone #: _____

Check the space on the left if item is in effect.

Administration:

____ **Complaints -** Designated contact person (the Privacy Officer) _____.
____ **Complaints -** Written procedures are established.
____ **Complaints** – Forms are available for clients.
____ **Documentation:** Arrangements made to keep for at least 6 years.
____ **Sanctions:** Written procedures for dealing with policy violations by your workforce.
____ **Training:** Documentation available of dates, places, or type of HIPAA-related training and who took it. Re-training should be documented, as well. Training should be specific to each job or position and take place before and during employment. Training should cover all aspects of HIPAA, State law and the Code of Ethics that are relevant to the person's job. Training must inform the staff of potential sanctions and remedial measures if they violate any rule or regulation.

Make sure your trainings cover all the policies and procedures required in the HIPAA Security Rule's three kinds of Safeguards for the workforce members who need to know them to do their jobs.

____ **Re-training:** Documentation available of interval and means of staff re-training.

____ **HIPAA File:** A special and separate repository (e.g. a folder, either electronic or real) was created to hold the forms, policies, account of training, reviews, complaints, etc., and all other HIPAA-related documentation.

Forms on File:

___ **Notice of Privacy Practices: This** form is to be signed by all clients prior to treatment.

___ **Display of Notice of Privacy Practices:** The Notice is displayed on (bulletin board, folder, website, waiting room, etc.):_____

___ **Acknowledgment of Receipt of Notice**

___ **Informed Consent and Office Policies:** This is a "pre-HIPAA" requirement. All clients prior to treatment must sign this form.

___ **Authorization to Release Information**

___ **Request for Amendment of Health Information**

___ **Standard Office Policies & Informed Consent**

___ **Tracking of Releases**

___ **Account of Disclosures**

___ **Denial of Access to PHI**

___ **Denial of Request for Amendment**

___ **Complaint form**

___ **Breach Assessment**

___ **Authorization to use unencrypted e-mail & text**

___ **Patient's Right for Confidential Communications**

___ **Patient request for restriction on use and disclosure of PHI**

Additional forms:

____

____

Physical Office Privacy:

____ No calling patients' last name in waiting room

____ No sign-in sheet for patients in waiting room

Release of records:

____ Before any release of records, the Privacy Officer, _____, verifies that the release is in keeping with HIPAA regulations and/or state law.

____ Records are carefully reviewed before being released; non-essential information is deleted; and only HIPAA-compliant "minimum necessary" information is released.
____ Records/logs of the releases are kept in detail (who sent it, why it was sent, when it was sent, and what was sent).
____ Written policy that describes how the above items are managed is in place, and includes an effective date when the policy starts and date when the policy is replaced or retired.
____ A procedure is in place to ensure that policies written regarding release of records are retained for 6 years after date of retirement.

Psychotherapy Notes:
____ I keep Psychotherapy Notes.
____ Clinical notations of Psychotherapy Notes are kept separately from the general records.
____ Psychotherapy Notes are separated from the general medical records by the following means **(e.g. separate, clearly marked folders; separate file cabinets; electronic record system separates and labels these notes as psychotherapy notes, etc.): _____**
____ Written policy that describes how psychotherapy notes are managed is in place, and includes an effective date when the policy starts and date when the policy is replaced or retired.
____ A procedure is in place to ensure that policies written regarding psychotherapy notes are retained for 6 years after date of retirement.

Complaints about privacy violations or privacy policy:
___ Protocols for handling complaints are in place
___ Anonymous reporting mechanism is in place
___ Protocol for investigating complaints is in place
___ Written policy that describes how complaints are managed is in place, and includes an effective date when the policy starts and date when the policy is replaced or retired.
___ A procedure is in place to ensure that policies written regarding complaints are retained for 6 years after date of retirement.

Documentation on File:
___ Security risk analysis completed and documentation of analysis is on file. The risk analysis is updated at least every year. (see Section XVI for helpful information on completing this item.)
___ Security risk management plan is written and on file. The risk management plan is updated every time the risk analysis is updated. (see Section XVI for helpful information on completing this item.)

___ Security Policies and Procedures manual is written and on file in a place where all workforce members can access it when needed. (see Section XVI for helpful information on completing this item.)

___ All Security policies and procedures include an effective date when the policy/procedure starts and date when the policy/procedure is replaced or retired.

___ A procedure is in place to ensure that all security policies and procedures are retained for 6 years after date of retirement.

___ A log/logs of security activities is kept for all regular activities. Logs are accessible at all times to workforce members who need access to them, and are protected from individuals who don't need to access them. Logs include (but are definitely not limited to) records of workforce training on privacy and security policies, software updates and upgrades, backups made, and any other activities performed to comply with the practice's own policies and procedures.

Business Associates (BA):
Copy and paste the following block for every third-party service provider you identify in your practice. Some therapists find it easier to make this list after they've completed their security risk analysis.

Name of third-party service provider: _____
Is provider a HIPAA Business Associate?
__Y __N
If yes, have you executed an up-to-date Business Associate Agreement (BAA) with them?
__Y __ N
If there is no BAA, explain the reasons for continuing to allow the BA to create, receive, maintain, or transmit PHI on your behalf:

Additional comments:

Form II:
Sample Business Associate Agreement Provisions

Insert your letterhead here

Words or phrases contained in brackets are intended as either optional language or as instructions to the users and should be modified according to the needs of the specific parties involved. This document includes language that is unlikely to apply to most solo practitioners. With the exception of entering the names of the covered entity (e.g name of the practice) and business associate. For most practitioners, much, if not all, of the additional content in green can be omitted.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the

business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that

such limitation may affect business associate's use or disclosure of protected health information.
(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.
(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.
(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]
(c) Obligations of Business Associate Upon Termination.
[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]
Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.
[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

I agree to the above terms of this agreement

Business Associate: _____ Date:_____
Signature: _____
Title: _____

Covered Entity: _____ Date: _____
Signature: _____
Title: _____

Form III:
HIPAA Notice of Privacy Practices

Before beginning treatment or assessment, CE MUST present this form to every patient. Patients' acknowledgement of receipt of this Notice is required.

IMPORTANT: The content of this form varies from state to state. (California Therapists: While the form is generally geared to California psychotherapists, you must still consult with your professional association and/or The California Office of HIPAA Implementation.)

Insert your letterhead here

HIPAA NOTICE OF PRIVACY PRACTICES

(Note to therapists: Section I below must appear in your Notice of Privacy Practices exactly as it appears hereunder.)

I. 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.

II. IT IS MY LEGAL DUTY TO SAFEGUARD YOUR PROTECTED HEALTH INFORMATION (PHI).

By law I am required to insure that your PHI is kept private. The PHI constitutes information created or noted by me that can be used to identify you. It contains data about your past, present, or future health or condition, the provision of health care services to you, or the payment for such health care. I am required to provide you with this Notice about my privacy procedures. This Notice must explain when, why, and how I would use and/or disclose your PHI. Use of PHI means when I share, apply, utilize, examine, or analyze information within my practice; PHI is disclosed when I release, transfer, give, or otherwise reveal it to a third party outside my practice. With some exceptions, I may not use or disclose more of your PHI than is necessary to accomplish the purpose for which the use or disclosure is made; however, I am always legally required to follow the privacy practices described in this Notice.

Please note that I reserve the right to change the terms of this Notice and my privacy policies at any time as permitted by law. Any changes will apply to PHI already on file with me. Before I make any important changes to my policies, I will immediately change this Notice and post a new copy of it in my office and on my website **(if applicable).** You may also request a copy of this Notice from me, or you can view a copy of it in my office or on my website, which is located at **(insert website address, if applicable).**

III. HOW I WILL USE AND DISCLOSE YOUR PHI.

I will use and disclose your PHI for many different reasons. Some of the uses or disclosures will require your prior written authorization; others, however, will not. Below you will find the different categories of my uses and disclosures, with some examples.

A. Uses and Disclosures Related to Treatment, Payment, or Health Care Operations Do Not Require Your Prior Written Consent. I may use and disclose your PHI without your consent for the following reasons:

1. For treatment. I can use your PHI within my practice to provide you with mental health treatment, including discussing or sharing your PHI with my trainees and interns. I may disclose your PHI to physicians, psychiatrists, psychologists, and other licensed health care providers who provide you with health care services or are otherwise involved in your care. Example: If a psychiatrist is treating you, I may disclose your PHI to her/him in order to coordinate your care.

2. For health care operations. I may disclose your PHI to facilitate the efficient and correct operation of my practice. Examples: Quality control - I might use your PHI in the evaluation of the quality of health care services that you have received or to evaluate the performance of the health care professionals who provided you with these services. I may also provide your PHI to my attorneys, accountants, consultants, and others to make sure that I am in compliance with applicable laws.

3. To obtain payment for treatment. I may use and disclose your PHI to bill and collect payment for the treatment and services I provided you. Example: I might send your PHI to your insurance company or health plan in order to get payment for the health care services that I have provided to you. I could also provide your PHI to business associates, such as billing companies, claims processing companies, and others that process health care claims for my office.

4. Other disclosures. Examples: Your consent isn't required if you need emergency treatment provided that I attempt to get your consent after treatment is rendered. In the event that I try to get your consent but you are unable to communicate with me (for example, if you are unconscious or in severe pain) but I think that you would consent to such treatment if you could, I may disclose your PHI.

B. Certain Other Uses and Disclosures Do Not Require Your Consent. I may use and/or disclose your PHI without your consent or authorization for the following reasons:

(Note to therapists: The following list is a compilation of federal and California laws)

1. **When disclosure is required by federal, state, or local law; judicial, board, or administrative proceedings; or, law enforcement.** Example: I may make a disclosure to the appropriate officials when a law requires me to report information to government agencies, law enforcement personnel and/or in an administrative proceeding.

2. **If disclosure is compelled by a party to a proceeding before a court of an administrative agency pursuant to its lawful authority.**
3. **If disclosure is required by a search warrant lawfully issued to a governmental law enforcement agency.**
4. **If disclosure is compelled by the patient or the patient's representative pursuant to California Health and Safety Codes or to corresponding federal statutes of regulations**, such as the Privacy Rule that requires this Notice.
5. **To avoid harm.** I may provide PHI to law enforcement personnel or persons able to prevent or mitigate a serious threat to the health or safety of a person or the public (i.e., adverse reaction to meds).
6. **If disclosure is compelled or permitted by the fact that you are in such mental or emotional condition as to be dangerous to yourself or the person or property of others, and if I determine that disclosure is necessary to prevent the threatened danger.**
7. **If disclosure is mandated by the California Child Abuse and Neglect Reporting law.** For example, if I have a reasonable suspicion of child abuse or neglect.
8. **If disclosure is mandated by the California Elder/Dependent Adult Abuse Reporting law.** For example, if I have a reasonable suspicion of elder abuse or dependent adult abuse.
9. **If disclosure is compelled or permitted by the fact that you tell me of a serious/imminent threat of physical violence by you against a reasonably identifiable victim or victims.**
10. **For public health activities.** Example: In the event of your death, if a disclosure is permitted or compelled, I may need to give the county coroner information about you.
11. **For health oversight activities.** Example: I may be required to provide information to assist the government in the course of an investigation or inspection of a health care organization or provider.
12. **For specific government functions.** Examples: I may disclose PHI of military personnel and veterans under certain circumstances. Also, I may disclose PHI in the interests of national security, such as protecting the President of the United States or assisting with intelligence operations.
13. **For research purposes.** In certain circumstances, I may provide PHI in order to conduct medical research.
14. **For Workers' Compensation purposes.** I may provide PHI in order to comply with Workers' Compensation laws.
15. **Appointment reminders and health related benefits or services.** Examples: I may use PHI to provide appointment reminders. I may use PHI to give you information about alternative treatment options, or other health care services or benefits I offer**.**
16. **If an arbitrator or arbitration panel compels disclosure,** when arbitration is lawfully requested by either party, pursuant to subpoena *duces tectum* (e.g., a subpoena for mental health records) or any other provision authorizing disclosure in a proceeding before an arbitrator or arbitration panel.
17. **If disclosure is required or permitted to a health oversight agency for oversight activities authorized by law.** Example: When compelled by U.S. Secretary of Health and Human Services to investigate or assess my compliance with HIPAA regulations.
18. **If disclosure is otherwise specifically required by law.**

C. Certain Uses and Disclosures Require You to Have the Opportunity to Object.

1. Disclosures to family, friends, or others. I may provide your PHI to a family member, friend, or other individual who you indicate is involved in your care or responsible for the payment for your health care, unless you object in whole or in part. Retroactive consent may be obtained in emergency situations.

D. Other Uses and Disclosures Require Your Prior Written Authorization. In any other situation not described in Sections IIIA, IIIB, and IIIC above, I will request your written authorization before using or disclosing any of your PHI. Even if you have signed an authorization to disclose your PHI, you may later revoke that authorization, in writing, to stop any future uses and disclosures (assuming that I haven't taken any action subsequent to the original authorization) of your PHI by me.

IV. WHAT RIGHTS YOU HAVE REGARDING YOUR PHI

These are your rights with respect to your PHI:

A. The Right to See and Get Copies of Your PHI. In general, you have the right to see your PHI that is in my possession, or to get copies of it; however, you must request it in writing. If I do not have your PHI, but I know who does, I will advise you how you can get it. You will receive a response from me within 30 days of my receiving your written request. Under certain circumstances, I may feel I must deny your request, but if I do, I will give you, in writing, the reasons for the denial. I will also explain your right to have my denial reviewed.

If you ask for copies of your PHI, I will charge you not more than $.25 per page. I may see fit to provide you with a summary or explanation of the PHI, but only if you agree to it, as well as to the cost, in advance.

B. The Right to Request Limits on Uses and Disclosures of Your PHI. You have the right to ask that I limit how I use and disclose your PHI. While I will consider your request, I am not legally bound to agree. If I do agree to your request, I will put those limits in writing and abide by them except in emergency situations. You do not have the right to limit the uses and disclosures that I am legally required or permitted to make.

C. The Right to Choose How I Send Your PHI to You. It is your right to ask that your PHI be sent to you at an alternate address (for example, sending information to your work address rather than your home address) or by an alternate method (for example, via e-mail instead of by regular mail). I am obliged to agree to your request providing that I can give you the PHI, in the format you requested, without undue inconvenience. I may not require an explanation from you as to the basis of your request as a condition of providing communications on a confidential basis.

D. The Right to Get a List of the Disclosures I Have Made. You are entitled to a list of disclosures of your PHI that I have made. The list will not include uses or disclosures to which you have already consented, i.e., those for treatment, payment, or health care operations, sent directly to you, or to your family; neither will the list include disclosures made for national security purposes, to corrections or law enforcement personnel, or

disclosures made before April 15, 2003. After April 15, 2003, disclosure records will be held for six years.

I will respond to your request for an accounting of disclosures within 60 days of receiving your request. The list I give you will include disclosures made in the previous six years unless you indicate a shorter period. The list will include the date of the disclosure, to whom PHI was disclosed (including their address, if known), a description of the information disclosed, and the reason for the disclosure. I will provide the list to you at no cost, unless you make more than one request in the same year, in which case I will charge you a reasonable sum based on a set fee for each additional request.

E. The Right to Amend Your PHI. If you believe that there is some error in your PHI or that important information has been omitted, it is your right to request that I correct the existing information or add the missing information. Your request and the reason for the request must be made in writing. You will receive a response within 60 days of my receipt of your request. I may deny your request, in writing, if I find that: the PHI is (a) correct and complete, (b) forbidden to be disclosed, (c) not part of my records, or (d) written by someone other than me. My denial must be in writing and must state the reasons for the denial. It must also explain your right to file a written statement objecting to the denial. If you do not file a written objection, you still have the right to ask that your request and my denial be attached to any future disclosures of your PHI. If I approve your request, I will make the change(s) to your PHI. Additionally, I will tell you that the changes have been made, and I will advise all others who need to know about the change(s) to your PHI.

F. The Right to Get This Notice by E-mail. You have the right to get this notice by e-mail. You have the right to request a paper copy of it, as well.

V. HOW TO COMPLAIN ABOUT MY PRIVACY PRACTICES

If, in your opinion, I may have violated your privacy rights, or if you object to a decision I made about access to your PHI, you are entitled to file a complaint with the person listed in Section VI below. You may also send a written complaint to the Secretary of the Department of Health and Human Services at 200 Independence Avenue S.W. Washington, D.C. 20201. If you file a complaint about my privacy practices, I will take no retaliatory action against you**.**

VI. PERSON TO CONTACT FOR INFORMATION ABOUT THIS NOTICE OR TO COMPLAIN ABOUT MY PRIVACY PRACTICES

If you have any questions about this notice or any complaints about my privacy practices, or would like to know how to file a complaint with the Secretary of the Department of Health and Human Services, please contact me at: **[insert therapist's name, address phone number, and e-mail].**

VII. NOTIFICATIONS OF BREACHES

In the case of a breach, **[Insert therapist's name]** requires to notify each affected individual whose unsecured PHI has been compromised. Even if such a breach was caused by a business associate, **[Insert therapist's name]** is ultimately responsible for providing the notification directly or via the business associate. If the breach involves more than 500 persons, OCR must be notified in accordance with instructions posted on its website. **[Insert therapist's name]** bears the ultimate burden of proof to demonstrate that all notifications were given or that the impermissible use or disclosure of PHI did not constitute a breach and must maintain supporting documentation, including documentation pertaining to the risk assessment.

VIII. PHI AFTER DEATH

Generally, PHI excludes any health information of a person who has been deceased for more than 50 years after the date of death. **[Insert therapist's name]** may disclose deceased individuals' PHI to non-family members, as well as family members, who were involved in the care or payment for healthcare of the decedent prior to death; however, the disclosure must be limited to PHI relevant to such care or payment and cannot be inconsistent with any prior expressed preference of the deceased individual.

IX. INDIVIDUALS' RIGHT TO RESTRICT DISCLOSURES; RIGHT OF ACCESS

To implement the 2013 HITECH Act, the Privacy Rule is amended. **[Insert therapist's name]** is required to restrict the disclosure of PHI about you, the patient, to a health plan, upon request, if the disclosure is for the purpose of carrying out payment or healthcare operations and is not otherwise required by law. The PHI must pertain solely to a healthcare item or service for which you have paid the covered entity in full. (OCR clarifies that the adopted provisions do not require that covered healthcare providers create separate medical records or otherwise segregate PHI subject to a restrict healthcare item or service; rather, providers need to employ a method to flag or note restrictions of PHI to ensure that such PHI is not inadvertently sent or made accessible to a health plan.)

The 2013 Amendments also adopt the proposal in the interim rule requiring **[Insert therapist's name],** to provide you, the patient, a copy of PHI if you, the patient, requests it in electronic form. The electronic format must be provided to you if it is readily producible. OCR clarifies that **[Insert therapist's name]** must provide you only with an electronic copy of their PHI, not direct access to their electronic health record systems. The 2013 Amendments also give you the right to direct **[Insert therapist's name]** to transmit an electronic copy of PHI to an entity or person designated by you. Furthermore, the amendments restrict the fees that **[Insert therapist's name]** may charge you for handling and reproduction of PHI, which must be reasonable, cost-based and identify separately the labor for copying PHI (if any). Finally, the 2013 Amendments modify the timeliness requirement for right of access, from up to 90 days currently permitted to 30 days, with a one-time extension of 30 additional days.

X. NPP

[Insert therapist's name] NPP must contain a statement indicating that most uses and disclosures of psychotherapy notes, marketing disclosures and sale of PHI do require prior authorization by you, and you have the right to be notified in case of a breach of unsecured PHI.

XI. EFFECTIVE DATE OF THIS NOTICE
This notice went into effect on Jan. 30, 2013

I acknowledge receipt of this notice

Patient Name: _____ Date:_____ Signature: _____

Patient Name: _____ Date: ____ Signature: _____

Form IV:
Authorization to Release Information

The content of this form may vary from state to state.
This form can replace the standard pre-HIPAA authorization or permission to release information.

Insert your letterhead here

AUTHORIZATION TO RELEASE INFORMATION

I, **(name of patient)** _____, (hereinafter "Patient") hereby authorize **(name of psychotherapist)** _____ , (hereinafter "Provider") to disclose mental health treatment information and records obtained in the course of psychotherapy treatment of Patient, including, but not limited to, therapist's diagnosis of Patient, to:

_____
_____

I understand that I have a right to receive a copy of this authorization. I understand that any cancellation or modification of this authorization must be in writing. I understand that I have the right to revoke this authorization at any time unless Provider has taken action in reliance upon it. And, I also understand that such revocation must be in writing and received by Provider at **(insert therapist's address)** _____ to be effective.

This disclosure of information and records authorized by Patient is required for the following purpose: _____
The specific uses and limitations of the types of medical information to be discussed are as follows **(be as specific as you choose to)**:

_____
_____

Such disclosure shall be limited to the following specific types of information:

_____
_____

Therapist shall not condition treatment upon Patient signing this authorization and Patient has the right to refuse to sign this form.

Patient understands that information used or disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and may no longer be protected by

the HIPAA Privacy Rule, although applicable California law may protect such information.

This authorization shall remain valid until: _____

Patient's signature: _____

Date:_____

Form V:
Request for Amendment of Health Information

Insert your letterhead here

REQUEST FOR AMENDMENT OF HEALTH INFORMATION

Date: _____
Patient name: _____
Birth date: _____ Phone: _____
Patient address: _____
Describe the information you would like to have amended:
_____
Date(s) of information to be amended (e.g., date of office visit(s):

_____

_____

What is your reason for making this request? (i.e., the information is incorrect, incomplete, or outdated) _____
_____

How is the information you want to amend incorrect, incomplete, or outdated?
_____
_____

What should the entry say (or not say) to be more accurate or complete?
_____
_____

Do you know of anyone who may have received or relied on the information in question (such as your doctor, health plan, or other health care provider)? Yes/No

If yes, please specify the name(s) and address(es) of the organization(s) or individual(s).

_____

Signature of patient or legal representative: _____

Date: _____

Form VI:
Tracking of Releases

The content of this form may vary from state to state.

Insert your letterhead here

Name of Patient	Date of Release	To Whom	Authorized by

Form VII:
Account of Disclosures

The content of this form may vary from state to state.

Insert your letterhead here

Patient Name _____

Accounting Time Period (max. 6 years): From _____ to _____

Here is the accounting of disclosures you requested.

As was articulated in the Notice of Privacy Practices, this document does not include disclosures made: (1) for treatment (e.g., if we referred you to another provider), (2) for payment (e.g., the claims filed with your health plan), (3) for health care operations (e.g., peer review of our work), (4) under any authorization that you signed, or (5) directly to you or your personal representative. There are additional exclusions to the disclosures we must account for.

For more information, contact our Privacy Officer, _____, at phone number: _____.

No disclosures were made that do not fall under one of the exclusions.

#1: Date of the Disclosure: _____
Person or Organization Receiving the Information: _____

Brief Description of the Information that was Disclosed:

_____

Purpose of the Disclosure:

_____

#2: Date of the Disclosure: _____
Person or Organization Receiving the Information: _____

Brief Description of the Information that was Disclosed:

_____

Purpose of the Disclosure:

_____

When available, we may include a copy of a written request for disclosure in lieu of the above items.

For a disclosure made more than once to the same recipient, the information above refers to the first disclosure.
The last disclosure made during this accounting period was on: _____

Form VIII:
Denial of Access to Protected Health Information (PHI)

This form may vary from state to state.

Insert your letterhead here

DENIAL OF ACCESS TO PROTECTED HEALTH INFORMATION (PHI)

Patient Name _____

Normally, my patients are allowed access to their Protected Health Information (PHI), and/or a copy of it, whenever they request it, but there are a number of instances where I may deny this access. By law, access to your PHI may be denied for any of the following indicated reasons. You may have access to any information that is not covered by any of the reasons below.

The following reasons <u>are not</u> subject to review:

☐ The information exists only in Psychotherapy Notes (which are the private notes written by your therapist).

☐ The information has been compiled in reasonable expectation of legal proceedings, or for use therein.

☐ The information was obtained from another party to whom I promised confidentiality. Allowing access would reveal that person's identity, which would be an ethical breach.

☐ This information was generated or maintained during treatment that is part of a research project. Since that research is still in progress, the information is not immediately available; however, when the research study is completed, you may have access to the information.

☐ The requested information is not in my possession. It is obtainable from _____.

☐ Because you are an inmate in a correctional institution, giving you access to this information could conceivably jeopardize the safety, health, security, rehabilitation, or custody of yourself or other inmates.

☐ You are an inmate of a correctional institution; therefore, access to this information might jeopardize the safety of an officer, staff member, or other person at this institution, or a person responsible for transporting you.

The following reasons <u>are</u> subject to review by a licensed health care provider, other than myself, in the event that you request a review of my decision.

- ☐ I believe that granting access to this information may possibly endanger the life or physical safety of you or another person.
- ☐ The information refers to another person (other than a health care provider) and it is possible that granting access to the information may cause significant harm to that person.
- ☐ You are the patient's personal representative and I believe that to grant you access would in all likelihood result in significant harm to that patient or some other individual.

How to Request a Review: Contact me directly if you would like to request a review of my decision. I will select a licensed health care professional to do the review and you will be notified of the decision. If the reviewer decides that access should be granted, I will grant it. If not, access will be denied.

Filing a complaint: Whether or not you request a review of my decision, you have the right to file a complaint against me. You may send your complaint directly to me, or, if you prefer, to my Privacy Officer:

Name and Number: _____

It is also your right to file a complaint with the Secretary of the U.S. Department of Health and Human Services. If you do, you must include my name and the nature of your complaint, i.e., denial of access. Your complaint must be written and must be sent within 180 days from the day of submission (although the Secretary may waive this time limit in some cases).

I regret that I cannot grant your request. I will be happy to discuss the matter with you at any time.

Sincerely,

Form IX:
Denial of Request for Amendment

This form may vary from state to state.

Insert your letterhead here

Denial of Request for Amendment

Patient Name _____

I try to ensure that the information in your records is complete and accurate. Nevertheless, mistakes can occur and, when they come to my attention, I correct them. You have requested that I amend your Protected Health Information (PHI). I cannot agree to amend your record for the reasons indicated hereunder.

☐ To the best of my knowledge, the information in your record is complete and accurate.
☐ You did not give enough information to make it clear that your records are incomplete or contain errors. Please provide me with any additional information you may have.
☐ The information you want to have amended is not part of the record that may be amended. The only part of the record that may be amended is that part containing your clinical and billing information or any part of the record used to make decisions about your care.
☐ The information is contained in the record that the law and other regulations do not permit you to access. Please see the attached document that explains why you cannot access the information.
☐ You did not request the amendment in writing, as required.
☐ Someone other than myself created the information you want to amend. Please send your request to the individual who created the information.

Your Rights If You Disagree with My Denial

If you disagree with my decision to deny the amendment, you are entitled to file a Statement of Disagreement in writing. Please submit it to my Privacy Officer or me:

Name and Number: _____

Note: A Statement of Disagreement must be reasonable in length. Also, I have the right to file a rebuttal to your Statement of Disagreement. If I do, I will ensure that you get a copy of my rebuttal.

A copy of your Statement of Disagreement and my rebuttal, or a summary of them, will accompany any future disclosure of the information in question.

If you do not wish to file a Statement of Disagreement, you still may request that I append a copy of your amendment request and a copy of my denial to this information whenever it may be disclosed in the future.

Filing a complaint

Whether or not you may request a review of my decision, it is still your right to file a complaint with me. It may be submitted directly to me, or to my Privacy Officer.

You also have the right to file a complaint with the Secretary of the U.S. Department of Health and Human Services. If you do, you must include my name and the nature of your complaint, i.e. denial of amendment. Your complaint must be in writing and must be sent within 180 days from the day of submission (although the Secretary may waive this time limit in some cases).

I regret that I cannot grant your request. I will be happy to discuss the matter with you at any time.

Sincerely,

Form X:
Complaint Form

This is a sample of a complaint form, primarily for complaints by patients with regard to privacy issues. For other types of complaints, you may need to use different kinds of forms. As always, adjust them, as necessary, to your specific situation, profession and state laws.

Insert your letterhead here.

Sample Complaint Form

Under HIPAA, you have the right to file a complaint with this office regarding our privacy practices, including our Notice of Privacy Practices and other privacy procedures. If you are not satisfied with your experiences here, we want to hear from you so that we can provide our services to you in ways that we both find satisfactory. You also have the right to file a complaint with the Secretary of the US Department of Health and Human Services at 200 Independence Ave. S.W. Washington, D.D. 20201.

If it is a clinical matter, we encourage you first to speak with your treating therapist. If it is an administrative-privacy concern, you can talk to our Privacy Officer, _____. If you are not satisfied or the problems still continues, please fill out this simple form and I assure you it will be investigated. We will try our best to fix it and to repair any damage that has been done. Also, I promise you that we will not in any way limit your care here or take any actions or retaliation against you if you bring a problem to our attention. You are entitled to receive a copy of this complaint.

Client's name _____ Date of birth _____

Identification No. _____ Telephone number _____

Client's address_____

What is or was the problem? _____

What would you like to see done about the problem? _____

Signature of client or his/her personal representative: _____
Date: ____

Printed name of client/personal representative: _____ Relationship to client: ___

Privacy Officer: _____ Phone: _____

Note: The Privacy Officer must respond to the client's complaint within 30 days from the time that s/he receives this form.

Form XI:
Acknowledgement of Receipt of Notice of Privacy Practice

There are a number of ways to document that patients have received the Notice of Privacy Practices. One way (the one I prefer) is to have the clients sign such an acknowledgement at the end of the Notice itself. Another way is to have a separate form such as the one provided below.

Insert your letterhead here

Acknowledgement of Receipt of Notice of Privacy Practice

I, _____, have received a copy of this Office's Notice of Privacy Practices.

Patient name: _____

Signature: _____ Date: _____

It is your right to refuse to sign this document

For Office Use Only:

The reason that a standard acknowledgment (such as the above) of the receipt of the Notice of Privacy Practices was not obtained:

_____ **Patient refused to sign.**

_____ **Communication barriers prohibited obtaining the acknowledgement.**

_____ **An emergency situation prevented this office from obtaining it.**

_____ **Others:** _____

Form XII:
Breach Assessment

Use this form to help you determine if a given security incident resulted in a "low probability of PHI compromise." In most cases, it may be necessary to consult with an expert to determine the answers to these questions. Answering them sometimes requires both technical knowledge and also knowledge of information system security issues. Before deciding on a final course of action after filling out this form, bring it to your attorney for guidance and advice.

Your security policies and procedures manual should contain a procedure that defines how you respond to security incidents. This form can be part of the procedure. Please note that the procedure should involve the early involvement of a qualified attorney so as to make sure you don't miss any ethically or legally required notifications during your process.

First: was the data "rendered unusable, unreadable, or indecipherable to unauthorized persons" at the time of the breach? Generally, full-device encryption with a strong encryption password is required to meet this condition. Consult with a security expert to be sure. **__Y __N**

If the answer is "Y," you may stop now. Bring the form to your attorney to confirm whether or not you need to perform any breach notification under HIPAA or state or local laws.

1. *The nature of the data that was misused or improperly disclosed:*
   - Did the data contain any personally identifying information about patients/clients? Refer to HIPAA's list of 18 identifiers for a list of things that can personally identify a patient/client. **__Y __N**
   - Is there a greater-than-low likelihood that the personally identifying data that was lost could be reasonably used to discover the identity of any patients/clients? **__Y __N**
2. *Who misused the information or received the unauthorized disclosure of the information:*
   - Are *any* of the persons who made an unauthorized misuse and/or who received the disclosed data still unidentified? **__Y __N**
     - If the answer is "Y," you must check "Y" for all other bullets under point 2.
   - Was the person(s) who made an unauthorized misuse and/or who received the disclosed data **NOT** someone who is a member of your workforce or a Business Associate? If they are such a person, are they **NOT** otherwise in compliance with applicable security policies and with HIPAA? **__Y __N**
   - Was the person(s) who made an unauthorized misuse and/or who received the disclosed data **NOT** a professional who is subject to privacy and security

laws? I.e. was it private individual, including a thief or other malicious actor? **__Y __N**

- Was the person(s) who made an unauthorized misuse and/or who received the disclosed data **NOT** a family member or caregiver of the affected patient(s) and trusted by the affected patient(s)? **__Y __N**

3. *Was there a chance for the breached PHI to be retained?*
   - Did the person(s) who made an unauthorized misuse and/or who received the disclosed data actually retain the data? (e.g. Did they get a copy or do they have ahold of the original? Did they have opportunity to memorize it?) **__Y __N**
     - If you don't know the answer, check "Y."
4. *How was the incident handled?*
   - Did the handling of this security incident fail to render compromise of the affected PHI unlikely, in a confirmable way? (e.g. did you fail to confirm that a smartphone thief was prevented from unlocking the stolen phone? Did you fail to confirm that a misdirected FAX was shredded before it was disclosed to unauthorized individuals? Etc.) **__Y __N**

There is no scoring rubric that can answer whether or not breach notification is necessary. This is why it is important to consult with someone with the necessary expertise to understand the outcomes of the security incident being assessed.

The more numbered points that are mostly "Y"s, however, the more likely it is that you will need to report.

If you choose not to report, the burden is on you to prove that your decision was reasonable. Retain all documentation of the security incident and of your breach assessment for the so long as you retain HIPAA documentation.

It is strongly advised that you bring any breach assessments to an attorney before deciding whether or not to perform a breach notification.

Form XIII:
Authorization to use unencrypted e-mail and text

This is a sample form for use with clients with whom you have performed a sufficiently rigorous process of discussing the security risks in e-mails or texts. The client has made it clear that s/he wants to use e-mail or texting despite the risks. You have collaborated on how to limit the use of e-mails and texts in ways that are necessary for the client's confidentiality. You have also confirmed that it is legal and ethical in your jurisdiction and under your codes of ethics.

It is strongly urged that this form not be used in telemental health practice contexts. You are also strongly urged to make sure you have sufficient knowledge of the risks involved in e-mail and texting before agreeing to use them with clients.

Insert your letterhead here

CONSENT TO USE UNENCRYPTED E-MAIL OR TEXT

It is very important that you are aware that computer e-mail, texts, and e-fax communication, can be relatively easily accessed by unauthorized people and hence can compromise the privacy and confidentiality of such communication. E-mails, texts, and e-faxes, in particular, are vulnerable to such unauthorized access due to the fact that servers or communication companies may have unlimited and direct access to all e-mails, texts and e-faxes that go through them. Generally, e-mails, text messages, and e-faxes are not encrypted in transit over the Internet. It is always a possibility that e-faxes, texts, and e-mail can be sent erroneously to the wrong address and computers. Unencrypted e-mail or texts provide as much privacy as a postcard. You should not communicate any information to your health care provider that you would not want to be included on a postcard that is sent through the Post Office. E-mail messages on your computer, your laptop, tablet computer, phone or other devices have inherent privacy risks – especially when your e-mail access is provided through your employer or school or when access to your e-mail messages is not well protected.

Please, note that e-mails, faxes, and texts are all part of your clinical records.

Please notify _____ [provider's name] if you decide to avoid or limit, in any way, the use of e-mail, texts, cell phone calls, phone messages, or e-faxes. If you communicate confidential or private information via unencrypted e-mail, texts or e-fax or via phone messages, it will be assumed that you have evaluated the risks and made an informed decision, _____ [provider's name] will view it as your agreement to take the risk that such communication may be intercepted, and your desire to communicate on such matters will be honored. Please do not use texts, e-mail, voice mail, or faxes for emergencies.

Patient's Name: _____
Cell Phone Number: _____
E-mail Address: _____
In case that authentication is needed, please give me a password _____
Patient's Signature: _____

Form XIV:
Patient's Right for Confidential Communication

Background note, this is not part of the form: *This form is in compliance with HHS Regulations Rights to Request Privacy Protection: Confidential Communications - § 164.522(b): A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations. ….A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.*

Insert your letterhead here

Patient Confidential Communications

The Health Insurance Portability and Accountability Act (HIPAA) gives you the right to request that **[provider's name]** communicates financial and/or medical information to you in confidence by a particular method or certain locations.

In order to protect the privacy and confidentiality of your information; please complete the following which tells me how you would like to be contacted.

I wish to be contacted in the following manner (check all that apply):

Phone Communications

____ Home Telephone Number _____

____ Work Telephone Number _____

____ Cell Phone Number _____

____ Do not contact me at home

____ Do not contact me at work

____ Leave message with your name and call-back # on answering machine

____ Leave message with medical information on answering machine

____ OK to give information to following family member(s), friend/s or co-workers, or others listed below

_____

Written Communication

___ Do not send written medical information to me

___ Mail information to my home address on file

___ Mail to my work/office address on file

___ Mail information to other address:

List _____

___ Fax to the following number _____

___ I do not want to communicate by E-mail

___ You can communicate via E-mail with me at _____

[provider's name] will continue to communicate with you according to your above response(s) until you change your preferences. You may do so by completing a new form.

By your signature below, you agree to be communicated in the above manner.

Patient Signature _____

Patient Name _____

Date _____

Form XV:
Patient requests for restriction and termination of restrictions on use and disclosure of PHI

Insert your letterhead here

Background note, this is not part of the form: *HIPAA regulations § 164.522(a) regarding right to request restrictions): Covered entities are required to give individuals the opportunity to request restrictions of the use and disclosure of protected health information by the covered entity. Patients have the right to revoke their request for restrictions.*

Patient request for restriction on use and disclosure of PHI

I request that **[therapist's name]** restricts the use and disclosure of protected health information (PHI) listed below. I understand that **[therapist's name]** may not agree to this request; provided, however, that **[therapist's name]** may be required by law to grant a restriction preventing disclosure to my health plan concerning services or items for which I have paid **[therapist's name]**.

Describe the restriction requested:

_____

_____

This restriction shall be in effect until (date or event):

_____

Patient Name, printed: _____

Signature: _____ Date: _____

Relationship if not patient: _____

Mailing Address for future correspondence regarding this restriction:

_____

[Therapist's name] has reviewed the above request to restrict the use and disclosure of protected health information (PHI) and ***(check one)***

__ Denies the request as **[Therapist's name]** cannot reasonably assure or guarantee the restriction can be met.

__ Accepts and will honor the request for the above stated restriction with the following exceptions and conditions:

- If you need emergency treatment and the restricted PHI is needed to provide emergency treatment, I may use the restricted PHI or may disclose this

information to another health care provider to provide you with the emergency treatment.
- I will ask the health care provider to not further use or disclose the PHI.
- To the extent permitted by law, I may need to terminate or revoke our acceptance of this restriction. Of course, I will notify you of such unilateral termination.

Therapist's Signature: _____ Date: _____

Title: _____

Revoking or Terminating Restrictions of Use and Disclosure of Protected Health Information

Check One:

____ **Patient:** I hereby ***revoke*** the above restriction of the use and disclosure of my protected health information (PHI) effective _____ (date).

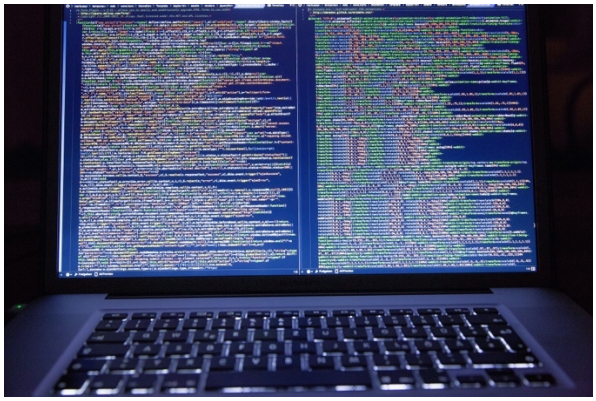
____ **[Therapist's name]** previously agreed to the above restriction of the use and disclosure of your protected health information (PHI). To the extent permitted by law, **[therapist's name]** ***terminates this previous agreement*** and no longer will restrict the use and disclosure of your protected health information effective _____ (date).

Signed: _____ Date: _____

Printed Name: _____

Relationship if not patient: _____

Section X
Risk Analysis and Security Policy & Procedure



As noted previously, it is incumbent on each organization to engage in ongoing risk analysis and security reviews. The extent and frequency will depend on the size of the organization. Many of the rules were written for larger organizations and did not have solo or small group practices in mind. Nonetheless, these requirements are written into HIPAA guidelines.

In addition to the HIPAA compliance checklist provided in form 1, the following link will take you to sections of a brochure published by the National Coordinator for Health Information Technology which can be used as guidance on maintaining compliance.

Privacy and Security Guide

References

Covered Entity Decision Tool. (2016). CMS.Gov. https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf

FAQs on Telehealth and HIPAA during the COVID-19 Nationwide Public Health Emergency. (2020). Hhs.Gov. https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

Health Information Privacy. (2022). Hhs.Gov. https://www.hhs.gov/hipaa/index.html

HHS ONC. (2015). Guide to Privacy and Security of Electronic Health Information. *https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf*

HIPAA Compliance Checklist 2022. (2022). HIPAA Journal. https://www.hipaajournal.com/hipaa-compliance-checklist/

HIPAA Security Series 2: Security Standards - Administrative Safeguards. (2007). Hhs.Gov. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

HIPAA Security Series 3: Security Standards - Physical Safeguards. (2007). Hhs.Gov. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

HIPAA Security Series 4: Security Standards - Technical Safeguards. (2007). Hhs.Gov. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

HIPAA Security Series 6: Basics of Risk Analysis and Risk Management. (2007). Hhs.Gov. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

Lustgarten, S., Garrison, Y., Sinnard, M., & Flynn, A. (2020). *Digital privacy in mental healthcare: Current issues and recommendations for technology use*. National Library of Medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7195295/?report=reader

New HIPAA Regulations. (2022). HIPAA Journal. https://www.hipaajournal.com/new-hipaa-regulations/

Office for Civil Rights. (2008, May 21). *Business Associate Contracts*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

Office for Civil Rights. (n.d.). Ocrportal.hhs.gov. https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

