*Overview*

**About Health Information Privacy and Security**

The privacy and security of health information are addressed through a patchwork of various federal and state laws. These laws are currently evolving, as Congress issues new legislation and the Department of Health and Human Services (HHS) promulgates regulations creating stricter protections and expanding the enforcement regime and related penalty structure. Further changes to the privacy and security regime are expected to take effect in February 2010, in the form of omnibus privacy regulations from HHS implementing changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regime made by the American Recovery and Reinvestment Act of 2009 (ARRA). Community health centers (centers) should continue to monitor shifting privacy and security requirements. Center’s Board of Directors, leadership, and staff all have responsibility for ensuring that centers comply with federal and state laws and regulations.

This section of the Manual provides a detailed summary of the key concepts and provisions in the HIPAA Privacy and Security Rules, and the HHS Data Breach Notification Rule. Additionally, this section of the Manual provides an outline of the privacy and security responsibilities of the center’s Board and leadership staff, as well as checklists to help ensure that centers are complying with applicable laws. Detailed privacy and security policies and procedures, as well as templates of relevant forms, are available in this Manual.

1. **Health Information Privacy And Security Overview**
2. **HIPAA Administrative Simplification**

HIPAA was the first comprehensive federal law to addresses the privacy and security of protected health information (PHI), as well as the simplification and standardization of transactions and identifiers.

1. The HIPAA Privacy Rule protects the confidentiality of all forms of PHI created or received by covered entities, including centers, by limiting use and disclosure without authorization. Compliance with the Privacy Regulations was required by April 14, 2003.
2. The HIPAA Security Rule specifies administrative, technical, and physical safeguards that are needed to protect the confidentiality electronic PHI (ePHI) maintained by covered entities, including centers. Compliance with the Security Regulations was required by April 20, 2005.
3. Covered entities needed to be able to send and receive electronic claims and other information in standard format, under the Electronic Transaction and Code Set Standards, by October 16, 2003;
   1. HIPAA required covered entities and healthcare providers who bill for services (e.g., centers and physicians) to obtain a National Provider Identifier (NPI) by May 23, 2007.
   2. The final regulations regarding HIPAA Administrative Simplification and Enforcement were issued on February 16, 2006.
4. **Expanded Privacy and Security Regime Through ARRA.** The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of ARRA, contains a number of amendments that expand the current HIPAA privacy and security protections and enforcement mechanisms. HHS regulations implementing ARRA’s privacy and security provisions are expected to be finalized by February 2010.
   1. Data Breach Notification Regulations. ARRA created new requirements for covered entities and business associates concerning the provision of notice to affected individuals if their unsecured PHI has been (or is reasonably believed to have been) accessed, acquired, or disclosed as a result of a breach. Depending on the circumstances, breach notification must be provided to individuals, HHS and/or the media. HHS established a harm threshold, which allows covered entities to forgo notification if they determine an incident poses little or no risk of financial, reputational or other harm to the individual. Although the Data Breach Notification regulations were effective as of September 23, 2009, HHS will not impose sanctions for failure to provide required notification about breaches that occurred before February 22, 2010.
   2. Texas Privacy and Security Laws. HIPAA preempts contrary or less restrictive state laws, but does not preempt state laws that provide greater privacy and security protections or rights.[[1]](#footnote-2) Centers need to comply with whichever provisions of either state or federal law provide patients with the greater protection. Centers located in Texas must comply with the provisions of the Texas Medical Records Privacy Act (TMRPA)[[2]](#footnote-3) to the extent that TMRPA is more restrictive or more protective of patients’ privacy than HIPAA. For example, TMRPA defines covered entity broader than HIPAA, and prohibits re-identification of PHI without prior written authorization, unlike HIPAA.[[3]](#footnote-4)
5. **Key HIPAA Privacy Terms And Provisions**
6. **Covered Entities.** HIPAA applies to covered entities such as health plans and health care clearinghouses, as well as to health care providers that engage in standard electronic transactions, generally including hospitals, pharmacies, and centers, among others. One important requirement is that the HIPAA privacy rule mandates that all covered entities, including covered centers, establish written policies and procedures to protect PHI. All center workforce members (i.e., employees, volunteers, trainees and others whose work is under the control of the center)[[4]](#footnote-5) must b be trained in and comply with HIPAA.
7. **Protected Health Information.** HIPAA restricts the use and disclosure of patients’ PHI, which includes:
   1. Information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
   2. Identifies the individual, or for which there is a reasonable basis for believing that the information can be used to identify the individual.
8. **Sensitive PHI.** Federal and state law provides special protections for certain kinds of particularly sensitive PHI.
   1. The HIPAA Privacy Rule and Texas law provide special protections for psychotherapy notes and patient mental health records.[[5]](#footnote-6) As a general rule, centers must obtain a separate authorization (i.e., on a separate form) to release patients’ psychotherapy notes, above and beyond a more general authorization to release PHI.
   2. To the extent centers evaluate or treat patients with chemical dependency, alcohol or drug abuse problems, they will need to comply with federal laws and regulations regarding the release of patients’ chemical dependency, alcohol or drug abuse records.[[6]](#footnote-7) As a general rule, centers must obtain a separate authorization to release patients’ chemical dependency, alcohol or drug abuse records, above and beyond a specific authorization to release PHI.
   3. Texas state law permits disclosure of patients’ HIV/AIDS information without authorization in the following limited circumstances:
      1. To the Texas Department of State Health Services (DSHS).
      2. To the federal Centers for Disease Control (CDC), state or local health authorities if such reporting is required by federal or state laws or regulations.
         1. To the physician or other healthcare provider who ordered the test.
         2. To physicians, nurses and other health care providers who have a legitimate need to know the test results for their protection and for the patient’s health and welfare.
         3. To the patient tested.
         4. To the spouse of the patient who tests positive for AIDS or HIV.
         5. To the patient’s partner, pursuant to a partner notification program when reported by a health care professional who actually knows that a patient is HIV positive and possibly has transmitted the HIV virus to a third party.
         6. To law enforcement officers, firefighters, emergency medical personnel, and correction officers exposed to the HIV virus, as provided by relevant law.
         7. To persons authorized to receive HIV test results obtained pursuant to Article 21.31 of the Texas Code of Criminal Procedure, which authorizes court-ordered testing of a defendant indicted for indecency with a child, sexual assault, or aggravated sexual assault.[[7]](#footnote-8)
      3. Under state law, genetic information is confidential and privileged regardless of the source of the information. The confidentiality of genetic information applies to a re-disclosure of genetic information by a secondary recipient of the information after disclosure of the information by an initial recipient.[[8]](#footnote-9) At the federal level, centers will need to consider the Genetic Information Nondiscrimination Act of 2008 (GINA).
   4. Limits on Use and Disclosure. The HIPAA privacy rule limits how centers may use and PHI for purposes other than treatment, payment, or health care operations. For all other purposes (subject to delineated exceptions, as described below), centers must obtain patients’ specific written authorization to release PHI. A sample authorization for use or disclosure of health information is provided in this manual.
   5. Use or Disclosure Permitted Without Authorization. The HIPAA Privacy Rule permits, but does not require, centers to use or disclose PHI without authorization for the following purposes:
      1. Uses and disclosures required by law.
      2. Uses and disclosures for public health activities (e.g., disease control and prevention, reports of child abuse, post-marketing surveillance).
      3. Disclosures about victims of abuse, neglect, or domestic violence.
      4. Uses and disclosures for health oversight activities.
      5. Disclosures for judicial and administrative proceedings (i.e., in response to a court order or subpoena).
      6. Disclosures for law enforcement purposes.
      7. Limited disclosures for identification and location purposes in response to a request by a law enforcement official (e.g., identification of suspects, missing persons, victims of a crime, decedents).
      8. Uses and disclosures about decedents.
      9. Uses and disclosures for cadaveric organ, eye, or tissue donation purposes.
      10. Uses and disclosures for research purposes.
      11. Uses and disclosures for specialized government functions (e.g., separation from military service, national security).
      12. Disclosures for workers’ compensation.

The HIPAA Privacy Rule specifies requirements and procedures for release of information subject to these exceptions. It is important to review an exception carefully to confirm that the use or disclosure you are considering actually fits within its confines, before moving forward.

* 1. Required Disclosures. The HIPAA privacy rule requires the center to disclose PHI in three instances:
     1. When the patient requests access to information about him or herself, or an accounting of certain disclosures, except as that right is limited by applicable law.
     2. When HHS requests information to investigate or determine the center’s compliance with the rules.
     3. When state law requires disclosure that is not prohibited by HIPAA.
  2. Business Associates. A business associate is a person or organization that receives, creates, or has access to PHI from or on behalf of a covered entity for the purpose of providing a function, activity, or service to that covered entity. Covered entities may release PHI to a business associate without authorization, but must have in place a written Business Associate Agreement, which contains a number of safeguards that are expressly mandated by regulations. A sample Business Associate Agreement is provided in this manual.
  3. Patient Rights. The HIPAA privacy rule establishes certain rights for patients whose PHI is maintained by covered entities. Centers must provide all patients who receive services from the center with notice of these limitations and rights in the form of a Notice of Privacy Practices. Specifically, patients have rights pertaining to access and amendment of PHI, restriction on disclosure of PHI, as well as a right to receive an accounting (i.e., a report) of certain disclosures of PHI. Sample policies and related forms are provided in this manual.
  4. Privacy Officer. The center must appoint a Privacy Officer to be responsible for developing, implementing, monitoring, and enforcing HIPAA privacy policies and procedures.
  5. Training. The center must ensure that all members of the center’s workforce receive initial training on HIPAA privacy policies and procedures, and are updated when the HIPAA privacy rule changes in any material way.
  6. Disciplinary Action. The center must take appropriate disciplinary action if it learns that a member of the center’s workforce has violated the HIPAA privacy rule, or the center’s HIPAA policies and procedures.

1. **Key HIPAA Security Terms And Provisions[[9]](#footnote-10)**
2. **Core Goals**. The HIPAA Security Rule ensures the confidentiality, integrity, and availability of electronic PHI (ePHI) created, received, maintained, or transmitted by covered entities. The HIPAA Security Rule seeks to protect against reasonably anticipated threats and hazards to the security or integrity of ePHI through a set of required and addressable (i.e., recommended) administrative, technical, and physical safeguards. The HIPAA Security Rule protects against privacy violations.
3. **General Framework.** The HIPAA Security Rule requires covered entities, including centers, to develop and implement policies and procedures addressing various standards. Some standards and implementation specifications are required (R), while others are addressable (A). Required actions must be taken. Addressable actions must be evaluated, in terms of whether they make sense in the entity’s environment, and the entity may either implement them or document the reasoning as to why they were not needed.
4. **Administrative Safeguards**
   1. Designated responsibility. Designate Information Security Officer (who may be the same as a Privacy Officer) to develop, implement, monitor, and enforce the center’s security policies and procedures (R).
   2. Security management. Prevent, detect, contain, and correct security violations (e.g., risk analysis (R), risk management (R), sanction policy (R), activity review (R)).
   3. Workforce security. Ensure workforce has appropriate access to ePHI and prevent those without access from obtaining ePHI (e.g., authorization/supervision (A), workforce clearance procedures (A), termination procedures (A)).
   4. Information management. Authorize access to ePHI (e.g., access authorization (A), access establishment and modification (A)).
   5. Security awareness. Train all members of workforce (e.g., security reminders (A), protection from malicious software (A), log-in monitoring (A), password management (A)).
   6. Security incident procedures. Identify and respond to security incidents (R), mitigating harmful effects (R).
   7. Contingency plan. Procedures for responding to an emergency or other occurrence that damages systems containing ePHI (e.g., data backup plan (R), disaster recovery plan (R), emergency mode operation plan (R), testing and revision procedures (A), applications and data criticality analysis (A)).
   8. Evaluation. Perform periodic technical and non-technical evaluations (R).
5. **Technical Safeguards**
   1. Access control. Systems that maintain ePHI should allow access only to those persons or programs that have been granted access (e.g., unique user identification (R), emergency access procedure (R), automatic log-off (A), encryption and decryption (A)).
   2. Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in systems that contain or use ePHI (R).
   3. Data integrity. Protect ePHI from improper alteration or destruction (e.g., authentication mechanisms (A)).
   4. Person or entity authentication. Verify that person or entity seeking access to ePHI has valid identity (R).
   5. Transmission security. Guard against unauthorized access to ePHI that is being transmitted electronically (e.g., integrity controls (A), encryption (A)).
6. **Physical Safeguards** 
   1. Facility access controls. Limit physical access to electronic information systems and facilities housing such systems (e.g., contingency operations (A), facility security plan (A), access control and validation procedures (A), maintenance records (A)).
   2. Workstation use. Specify proper functions to be performed at a workstation (includes laptops, desktops, PDAs, etc.) (R).
   3. Workstation security. Implement safeguards to restrict access to authorized users (R).
   4. Device and media controls. Policies and procedures governing receipt and removal of hardware and electronic media with ePHI from facility, and movement of these items within facility (e.g., disposal (R), media re-use (R), accountability (A), data backup and storage (A)).
7. **Disciplinary Action.** The center must take appropriate disciplinary action if it learns that a member of the center’s workforce has violated the HIPAA privacy rule, or the center’s HIPAA policies and procedures.
8. **Key HIPAA Data Breach Notification Terms And Provisions[[10]](#footnote-11)**
9. **Breach.** A breach means the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the HIPAA privacy rule, which compromises the security or privacy of the PHI.
10. **Safe Harbor:** **Secured PHI**. Importantly, the HHS breach notification requirements only apply to unsecured PHI. Breaches involving data that has been secured (i.e., rendered unusable, unreadable, or indecipherable to unauthorized individuals through encryption or destruction, in the manner set forth by HHS) are not subject to the notification requirement.
11. **Harm Threshold.** HHS interpreted the statute to allow covered entities to forgo notification if they determine that an incident poses little or no risk of financial, reputational, or other harm to the individual whose PHI was involved (i.e., in terms of the definition of breach, the incident did not compromise the security or privacy of the information).
12. **Risk Assessment.** Under this standard, the center must perform a fact-specific risk assessment to determine whether a breach occurred. The center should document the risk assessment. HHS described several factors that covered entities and business associates should consider in their risk assessments, including:
    1. Considering who received the PHI (e.g., a hacker versus a hospital or pharmacy).
    2. Any mitigation efforts that may reduce the likelihood of harm; whether the PHI (or media storing the PHI) was returned prior to access or use.
    3. The nature of the PHI disclosed.
13. **Exceptions from What Constitutes a Breach:**
    1. Any unintentional acquisition, access, or use of PHI by a center’s workforce member or person acting under the authority of a center or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy regulations.
    2. Any inadvertent disclosure by a person who is authorized to access PHI at the center or Business Associate to another person authorized to access PHI at the same center or Business Associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy regulations.
    3. A disclosure of PHI where the center or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
14. **De-Identified Data.** Use or disclosure of PHI that has been stripped of identifiers as set forth in the HIPAA Privacy Rule does not compromise the security or privacy of the information, and breach notification would not be required in the event an incident occurred. The following identifiers must be removed from data for it to be de-identified:
    1. Names.
    2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo-codes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
    3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
    4. Telephone numbers.
    5. Fax numbers.
    6. Electronic mail addresses.
    7. Social security numbers.
    8. Medical record numbers.
    9. Health plan beneficiary numbers.
    10. Account numbers.
    11. Certificate/license numbers.
    12. Vehicle identifiers and serial numbers, including license plate numbers.
    13. Device identifiers and serial numbers.
    14. Web Universal Resource Locators (URLs).
    15. Internet Protocol (IP) address numbers.
    16. Biometric identifiers, including finger and voice prints.
    17. Full face photographic images and any comparable images.
    18. Any other unique identifying number, characteristic, or code, except as permitted by section.
    19. In addition, the covered entity must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.
15. **Unsecured PHI.** PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through encryption or destruction. Redacted PHI is considered unsecured PHI.
16. **Notification of Individuals**
    1. A center must notify affected individuals without unreasonable delay but in no case later than 60 days after a breach is discovered.
       1. A breach is considered to be discovered by the center on the first day on which such breach is known, or should reasonably have been known (through the exercise of reasonable diligence) to the center, a member of the center’s workforce, or an agent of the center.
       2. If a breach is discovered by a business associate who is an agent of the center (as defined by federal common law), the breach will be considered to be discovered by the center on the first day that the business associate discovered the breach, regardless of when the business associate actually reports the breach to the center.
       3. If a breach is discovered by a business associate who is an independent contractor of the center, the breach will be considered to be discovered by the center on the first day that the Business Associate reported the breach to the center.
    2. The Notification should include, to the extent possible, the following information, set forth in plain language:
       1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
       2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
       3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
       4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
       5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.
    3. The center must notify affected individuals by written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.
       1. Notification may be provided in one or more mailings as information is available.
       2. If the center knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail may be provided to either the next of kin or personal representative of the individual.
    4. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual, the center may use a substitute form of notice reasonably calculated to reach the individual.
       1. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
       2. If the center has insufficient or out-of-date contact information for fewer than 10 individuals, the center can provide notice by telephone, or other means.
       3. If the center has insufficient or out-of-date contact information for 10 or more individuals, the center must provide substitute notice:
          1. Through a conspicuous posting for a period of 90 days on the center’s website or in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
          2. Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual’s unsecured PHI may be included in the breach.
       4. If the center deems that a situation requires urgency because of possible imminent misuse of unsecured PHI, the center may provide information to individuals by telephone or other means, as appropriate, in addition to written notice.
17. **Notification to Media**
    1. If a breach involves more than 500 Texas residents, the center shall notify prominent media outlets serving Texas without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
    2. Notification to the media must contain the same information as notification to the individual. The Notification shall not contain any PHI.
18. **Notification to Secretary**
    1. For breaches involving 500 or more individuals, the center must notify the Secretary of Health and Human Services (Secretary) through the [U.S. Department of Health & Human Services](http://transparency.cit.nih.gov/breach/index.cfm.) website.
    2. For breaches involving fewer than 500 individuals, the Center shall maintain a log or other documentation of such breaches and submit notification of the breaches to the Secretary through the [U.S. Department of Health & Human Services](http://transparency.cit.nih.gov/breach/index.cfm) website.
19. **Federal Data Breach Guidance.** Additional guidance about data breach notification requirements for covered entities is available at the [U.S. Department of Health & Human Services](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html) website.
20. **Key HIPAA Transactions, Code Sets, And National Provider Identifiers Terms And Provisions**
    1. **Standard Transactions.** The term standard transactions includes various electronic transactions (e.g., relating to claims processing) HHS has identified that must be conducted in a standard format (i.e., including certain data elements). The goal is to simplify the billing process and to provide protection from unauthorized disclosure of PHI.
    2. **Code Sets.** The term code sets means codes to identify diagnosis, treatment or other health services for purposes of billing and tracking. Code Sets that must be used are the standard service codes including International Statistical Classification of Diseases and Related Health Problems or ICD-9-CM[[11]](#footnote-12) (diagnoses and procedures), Current Procedural Terminology or CPT-4 (procedures and services), Healthcare Common Procedure Coding System or HCPCS (adjunct to CPT-4), Code on Dental Procedures and Nomenclature or CDT-2 (dental services) and National Drug Code (NDC) (pharmacy transactions). Note that code sets may be updated annually, so it is necessary to secure the current code sets to use for billing purposes. Sources of Information on these code sets are as follows:
       1. ICD-9-CM; [Government Printing Office](http://www.gpo.gov) (202-512-1800).
       2. CPT-4; American Medical Association and other private sources.
       3. [HCPCS](http://www.cms.gov/medicare/hcpcs).
       4. CDT-2; American Dental Association (1-800-947-4746).
       5. [NDC](http://www.fda.gov/cder/ndc/index.htm).
    3. **National Provider Identifiers (NPI).[[12]](#footnote-13)** The final rule on Standard Unique Health Identifier for Health Care Providers was issued, on January 23, 2004. These HIPAA Regulations require that Unique Identifiers (National Provider Identifiers or NPIs) be established for all employers, healthcare providers, and health plans.[[13]](#footnote-14) The NPI will be used when processing claims for Medicare, Medicaid and private health insurance. Compliance for centers and their healthcare providers who bill for services was required by May 23, 2007.[[14]](#footnote-15) The NPI is used when processing claims for Medicare, Medicaid and private health insurance.
21. **HIPAA and ARRA Enforcement And Penalties**
    1. **Enforcement.** HIPAA enforcement began as more of an outreach and education effort, supplemented by a complaint-driven process, with rare egregious cases being referred to the U.S. Department of Justice for criminal prosecution. ARRA reflects a marked change in enforcement philosophy. Authority to enforce HIPAA Privacy and Security components is now consolidated under the HHS Office for Civil Rights (rather than shared with CMS).[[15]](#footnote-16) Significantly, ARRA created multiple new enforcement mechanisms and tools, which will be phased in over the next few years, including:
       1. Authorizing State Attorneys General (AGs) to bring civil actions in federal district court in cases where they believe that state residents are harmed by a HIPAA violation; State AGs may seek statutory damages, injunctive relief and attorney fees.
       2. Requiring the Secretary of HHS to conduct periodic audits of covered entities and business associates.
       3. Requiring the Secretary of HHS to investigate complaints and impose CMPs where a violation is be due to willful neglect (corrective action plans will remain an option where there is no finding of willful neglect).
       4. Civil monetary penalties (CMPs) collected for violations are to be shared with OCR to fund HIPAA enforcement and also possibly with harmed individuals.
    2. **Penalties.** ARRA dramatically expanded the HIPAA penalty regime and extended it to apply directly to business associates. Before ARRA, violations carried a penalty of not more than $100 per violation, with an aggregate limit of $25,000 for all violations of an identical requirement or prohibition during a calendar year.
       1. Civil Penalties. ARRA created a tiered penalty regime with a maximum penalty of $1.5 million per year. Penalties are based on: whether or not a Covered Entity (including physicians) knew of a breach of privacy; whether the breach was due to reasonable cause and not willful neglect; or whether the breach was due to willful neglect. The Secretary has discretion to determine the amount of penalty based on the nature and extent of the violation and the extent of the harm resulting from the violation.
22. Unknowing violation - $100 per violation, not to exceed $25,000 per year.
23. Reasonable cause - $1,000 per violation, not to exceed $10,000 per year.
24. Willful neglect - if corrected, $10,000 per violation, not to exceed $250,000 per year.
25. Willful neglect - if not corrected, $50,000 per violation, not to exceed $1.5 million per year
    * 1. Criminal Penalties. Under ARRA, criminal penalties can range up to $50,000 and 1 year in prison for certain offenses; up to $100,000 and up to 5 years in prison if the offenses are committed under false pretenses; and up to $250,000 and up to 10 years in prison if the offenses are committed with the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm. ARRA expressly applies HIPAA criminal penalties to business associates and to employees of covered entities.
26. **HHS Guidance**
    1. **Privacy Guidance.** HHS has issued guidance to assist covered entities in complying with the HIPAA Privacy Regulations, including a searchable collection of frequently asked questions. These materials are available at the [U.S. Department of Health & Human Services](http://www.hhs.gov/ocr/privacy/) website.
    2. **Security Guidance.** HHS has issued a series of technical guidance documents to assist covered entities in complying with the HIPAA Security Regulations. These materials are available at U.S. Department of Health & Human Services [Center for Medicare & Medicaid Services](http://www.cms.gov/HIPAAGenInfo/04_PrivacyandSecurityStandards.asp).
27. **Board Responsibility For Protecting Patient Privacy**
    1. **Role of the Board.** While key persons (such as the Privacy Officer) at the center will be designated to oversee HIPAA issues, all workforce members are responsible for knowing and acting consistently with the center policies and procedures regarding privacy, security, and data breach notification compliance. The Board’s role is to ensure that appropriate policies and procedures are in place, that all workforce members are aware of, and trained in, such policies and procedures, and that the center’s daily operations are based on the policies and procedures.
    2. **Designation of Privacy Officer/Information Security Officer**. The Board is responsible for appointing a point-person to oversee the center’s compliance with the HIPAA Privacy and Security Rule, and the Data Breach Notification Rule. Depending on the size of the center, these roles can be filled by the same individual.
       1. Core responsibilities would likely include monitoring the impact of pending regulatory changes; developing internal policies, procedures, and related forms to comply with contractual and legal obligations; and addressing any privacy or security concerns that may be raised by patients or workforce members.
       2. Smaller centers may choose to assign these duties to an existing staff person, such as an office manager, and larger centers may create one or more full-time privacy and security positions.
    3. **Policies and Procedures.** The Board is responsible for ensuring that the center’s policies and procedures comply with applicable federal, state and local laws and regulations, including HIPAA. Center HIPAA policies and procedures must be adopted and/or incorporated into the various existing center policies and procedures. Policies and procedures must be updated to reflect changes in the law; TACHC will provide guidance regarding such changes. The Board must ensure that the center’s HIPAA policies and procedures, include, at a minimum:
       1. Privacy:
          1. Appointment of a HIPAA Privacy Officer.
          2. Business Associates.
          3. Notice of Privacy Practices.
          4. General Use and Disclosure of PHI.
          5. Patients’ Right to Access Records.
          6. Patients’ Requests for Amendments.
          7. Accounting of Disclosures of PHI.
          8. Patients’ Requests for Additional Privacy.
          9. Patient Complaints.
          10. Disciplinary Action.
          11. Training.
       2. Security:
          1. Administrative safeguards.
          2. Technical safeguards.
          3. Physical safeguards.
          4. Disciplinary actions.
       3. Data Breach Notification:
          1. Risk assessment.
          2. Notice to individuals.
          3. Notice to media.
          4. Notice to Secretary.
          5. Documentation
    4. **Workforce Training**. HIPAA requires that Centers (as Covered Entities) train all workforce members (which is defined broadly) regarding compliance with Policies and Procedures. The Center should include HIPAA Compliance Training in the Center’s Personnel Policies and Procedures.
    5. **Business Associate Agreements**. The Governance Board should ensure that Centers execute written Business Associate Agreements with all Vendors and Contractors. The Center’s Privacy Officer should maintain a current list of the Center’s Business Associates and copies of all executed Business Associate Agreements.

1. See [Texas OAG analysis](https://www.oag.state.tx.us/notice/hipaa.pdf) of what is pre-empted in state law by HIPAA. [↑](#footnote-ref-2)
2. Texas Health and Safety Code §181.001, as amended from time to time. [↑](#footnote-ref-3)
3. Texas Health and Safety Code §181.151 [Re-identified Information]. [↑](#footnote-ref-4)
4. See 45 CFR §160.103. [↑](#footnote-ref-5)
5. Texas R. Evid. §510 [Patient – Professional Privilege]; Texas Health and Safety Code §611.001-.008. [Mental Health Records]. [↑](#footnote-ref-6)
6. 42 USC §290dd-2; 42 CFR, Part 2, §2.31 [Alcohol and Drug Abuse Records], as amended from time to time. [↑](#footnote-ref-7)
7. See Texas Health and Safety Code Chapter 81, §81.001 [Communicable Diseases]. [↑](#footnote-ref-8)
8. Texas Occupations Code Chapter 58, Subchapter C, § 58.102; Texas Labor Code §21.403 [Employers]; 45 CFR §164.508(a)(1) [Disclosure for Genetic Counseling under HIPAA]; See generally, Texas Occupations Code §159.002(c)) [Regarding “Confidential Communications” between Physician and Patient, re-disclosure of confidential health information is prohibited except to the extent the disclosure is consistent with the authorized purposes for which the information was first obtained]. [↑](#footnote-ref-9)
9. Public Law 104-191 (104th Congress). HIPAA is codified at 42 US. §1320d – 1320d-8, and its regulations, including the “Standards for Privacy of Individually Identifiable Protected Health Information” (Privacy Regulations) and the “Security Standards for Electronic Protected Health Information” (Security Regulations) are codified at 45 CFR Parts 160, 162 and 164 (collectively, “the Privacy and Security Regulations” or HIPAA). [↑](#footnote-ref-10)
10. The Texas Identity Theft Enforcement and Protection Act requires businesses, including health care providers, disclose unauthorized acquisition of computerized data – including information that identifies an individual and relates to the individual’s physical or mental health, provision of health care to the individual, or payment for the provision of health care to the individual – that compromises the security, confidentiality, or integrity of such information to affected individuals as quickly as possible. The Texas state law does not explicitly contain a harm threshold, and could be construed to require disclosure of all unauthorized acquisition, regardless of the risk of harm to the affected individual. HIPAA generally preempts “contrary” provisions of state law. A state law is contrary when “a Covered Entity would find it impossible to comply with both the State and federal requirements, or the provision of state law stands as an accomplishment and execution of the full purposes and objectives” of HIPAA. 45 CFR §160.201. Although, as discussed above, the HIPAA Privacy Rule does not preempt state laws that offer more protections for patient privacy rights, HHS explicitly said that this exception applies only to the Privacy Rule and does not apply to the Data Breach Notification Rule. Breach Notification for Unsecured Protected Health Information (Interim Final Rule), 74 Federal Regulation 42,740, 42,576 (Aug. 24, 2009). The Texas could arguably be preempted because it does not contain a harm threshold and thus imposes burdens on Covered Entities that the federal law intended to remove. However, as this area of privacy law is still developing, it is unclear that the preemption argument would be successful. Centers should contact their local counsel for additional guidance in case of data breach. [↑](#footnote-ref-11)
11. ICD-9 will soon convert to ICD-10. Compliance date as of 3.15.2012 is 10.1.2013. Please see ICD-10 training modules on CHLN.org for more information. [↑](#footnote-ref-12)
12. 45 CFR Part 162. [↑](#footnote-ref-13)
13. The regulations pertaining to the use of a NPI has various effective dates of compliance: The Employer Identification Number (EIN) issued by the Internal Revenue Service (IRS) was selected as the identifier for employers on standard transactions, effective July 30, 2002. However, Centers and Physician providers must obtain a NPI by May 23, 2007. The unique identifier for health plans is pending. [↑](#footnote-ref-14)
14. 45 CFR §162.402. [↑](#footnote-ref-15)
15. Prior to July 2009, CMS enforced the Security Rule while OCR enforced the Privacy Rule. On July 27, 2009, the Secretary of HHS delegated authority to OCR to enforce both HIPAA Rules. [↑](#footnote-ref-16)