HIPAA Basics—
Understanding the Federal Regulations
HIPAA Basics—Understanding the Federal Regulations

Weston Distance Learning®
020WDLGSP02A-82
Acknowledgments

Author
Deborah Helmers

Editorial Staff
Trish Bowen
Katy Little
Lindsay Hansen
Bridget Tisthammer
Melissa Meltzer
Ryan Johnson
Courtney Sanderson
Brenda Blomberg

Design/Layout
Connie Hunsader
Sandra Petersen
D. Brent Hauseman

Weston Distance Learning, Inc.
Fort Collins, CO
www.westondistancelearning.com
HIPAA Basics: Understanding the Federal Regulations

HIPAA and You

As you move into your career as a healthcare professional, you will likely often hear the word HIPAA. We’ve mentioned HIPAA several times throughout your course of study. Now, let’s take a closer look at just what HIPAA is and what it means for you.

This supplement is designed to give you a general overview of HIPAA. Federal regulations as a whole and the HIPAA regulations in particular are not known for their simplicity of language and straight-forwardness. There is a lot of misinformation and confusion on this topic. It will be to your advantage to be armed with the facts as you interview for employment and talk to other healthcare professionals. Simply in terms of your own professional development, it is essential that you have a good grasp on the basics of this important legislation.

If you work as an employee in the healthcare field, your employer probably has instituted a HIPAA compliance program. All you need to do is get on board and follow the procedures and policies put in place. If you work independently, you will be in charge of upholding your end of the HIPAA responsibility.

As you read, keep in mind that this supplement is also an overview of HIPAA as a whole. Don’t feel overwhelmed. Through your coursework, you already are familiar with many of HIPAA’s most basic concerns: ethics, privacy, confidentiality and security of records.

Let’s start with a look at the HIPAA story!

What Is HIPAA?

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). This act has two main objectives. The first objective (portability) is to ensure the continuation of health insurance coverage for workers and their families during times of job change or loss. The second (accountability) is to increase the effectiveness of the healthcare system while protecting health data integrity, confidentiality and availability and preventing fraud and abuse.

Many experts call HIPAA the most sweeping healthcare legislation in the last 30 years. Its provisions touch nearly everyone who works in health care. Providers, payers, billers, coders, transcriptionists, clearinghouses—anyone who deals with confidential patient information is affected.

The different sections of HIPAA are known as titles. It is Title II, Subtitle F, that is probably the most important to the HIM professional. This part is called Administrative.
Simplification. When healthcare professionals talk about HIPAA and being HIPAA compliant, they are usually referring to this section.

HIPAA:

1. Ensures the continuation of health insurance coverage for workers who change or lose their jobs.
2. Increases healthcare effectiveness and protects data integrity, confidentiality and availability.

The HITECH Act
In February 2009, Congress passed the American Recovery and Reinvestment Act (ARRA). Within ARRA was Title XIII, the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act made some important revisions to the original HIPAA legislation, effective February 2010. HITECH expanded responsibilities for security and made other changes relating to the disclosure of protected health information (PHI) and enforcement of regulations.

Administrative Simplification
People in the healthcare industry have long recognized the problems that arise from variations in how its many segments do business. The HIPAA Administrative Simplification legislation addresses the lack of consistency.

Congress gave the healthcare industry a specified amount of time to establish standards in certain problem areas. Since the industry did not come to a consensus before the deadline passed, the legislation mandated that the responsibility of setting standards default to the Department of Health and Human Services (also known as the HHS or DHHS). The HHS, then, wrote the Administrative Simplification rules. You may think that HIPAA just means more confusion and work. In fact, however, the goal of the Administrative Simplification portion of HIPAA is—amazingly—to simplify your job.

Administrative Simplification (HIPAA Title II, Subtitle F) sets up nationally consistent regulations in four main areas: electronic transactions, privacy, security and identification numbers.

The Four Rules of Administrative Simplification

- Electronic Transaction Standards Rule
- Privacy Standards Rule
- Security and Electronic Signature Standards Rule
- Standard Identifiers Rule

We’ll examine each rule of HIPAA’s Administrative Simplification in more detail in a moment. First, let’s look at what types of businesses and entities fall under the HIPAA
Covered Entities

HIPAA affects virtually everyone in the healthcare field. Any provider or professional who transmits healthcare information in electronic form must comply with the new rules. HIPAA also covers all health plans and healthcare clearinghouses. These three main groups—providers that transmit health information electronically, health plans and healthcare clearinghouses—are known as **covered entities**. For the purposes of the security rule only, the term covered entity also includes a provider that maintains health information electronically, regardless of whether that entity transmits the information electronically.

HIPAA’s regulations also reach to those who do business with covered entities. This includes billing agencies, service organizations and all other **business associates**.

As of February 2010, under the provisions of HITECH, business associates are directly subject to HIPAA rules, enforcement and penalties in exactly the same way as covered entities. This is one of the changes from the original HIPAA legislation, which held only covered entities directly responsible.

**Who Must Comply?**

**Covered Entities**

- Providers, including hospitals, nursing homes, physicians and laboratories, that transmit (all Rules) or maintain (Security Rule only) healthcare information electronically.
- Health plans, including traditional insurance, managed care, government programs and other healthcare payers.
- Clearinghouses, third-party administrators
- Business Associates of any covered entity.

Of course, there are exceptions to every rule. Here are the few entities that HIPAA does not cover:

- Telecommunications companies and Internet service providers
- Group health plans, administered internally, with fewer than 50 participants
- Workers’ compensation plans
- Some liability plans and government agencies

**Electronic Transaction Standards Rule**

As you know, many patients do not pay for their medical care directly. Rather, a third-party payer system is the source of revenue for most medical care providers. The payer system used to be composed of a multitude of private companies and government...
agencies that each had their own preferred method of receiving and paying claims. There used to be about 400 different formats for healthcare claims. No wonder claims were often returned or denied!

The **Electronic Transaction Standards Rule** set both the formats for and the specific codes that were to be used in insurance claims. As of the compliance date—October 16, 2003—all healthcare businesses are required to use the same format for the same type of transaction. In other words, regardless of provider or payer, one single format is used for all claims, another format for all referrals and authorizations and yet another for all payments. In all, 10 standard formats were chosen. These cover all aspects of the healthcare industry.

Let’s take a closer look at some of the components of the Electronic Transaction Standards Rule.

**How Does HIPAA Define Electronic?**

According to the Electronic Transaction Standards Rule, a transaction is **electronic** if it is transmitted with an electronic medium. This includes the Internet, Extranet, leased lines, dial-up lines and private networks. Information physically moved from one location to another with storage media, such as magnetic tapes, disks or CDs, is also considered an electronic transaction. HIPAA standards do not cover telephone voice response and faxback systems.

**Electronic Media**

- Internet (public)
- Extranet (semi-private; authorized public users can access portions of a company’s private network)
- Leased lines
- Dial-up lines
- Private networks
- Storage devices (magnetic tapes, disks, CDs) physically moved from one location to another

**What Is a Transaction?**

According to HIPAA, a **transaction** is the transmission of information between two parties to carry out financial or administrative activities that occur in a medical facility or office other than those related to treatment. HIPAA standards clearly define which transactions must be compliant with the Electronic Transaction Standards Rule and have developed new formats for those transactions. These are listed here.
Under HIPAA, all providers, payers and clearinghouses that transmit electronically have to use the same standard format to send and receive the listed transactions. Each entity must accept the same format and cannot ask for additional information not already contained in the standard.

The Benefits of Using Electronic Transaction Standards

It’s important to remember that HIPAA doesn’t require that providers submit electronically. It only requires that those transactions that are sent electronically use the electronic transaction standards. A provider still will be able to use the CMS-1500 form to submit paper claims. However, all electronic claims must be ASC X12 837.

There are some real benefits to submitting claims electronically. Let’s look at some of these advantages of Electronic Data Interchange (EDI):

- **Unnecessary re-entering of data is prevented with electronic data transactions.** Each time data are processed manually (such as when secondary claim forms are filed), it represents a significant cost in wages and resources. EDI can result in faster transfer of data, fewer errors, less time wasted handling exceptions and a more streamlined business process.

- **The likelihood of errors is decreased.** Manually entering data—particularly entering the same data repeatedly—can result in errors that may not be detected until business or patient health consequences bring the error to your attention.

- **EDI is faster and cheaper than mailing.** The time and expense of mailing paper claims is another reason EDI is attractive. Average mail delivery times can vary from one to several days for normal, first-class mail. There is also some degree of uncertainty as to whether a mailed form will be received at all.

- **EDI eliminates the need to stockpile paper claims.** Another benefit of EDI is that it eliminates the need to stock and maintain an inventory of the various forms required to file paper claims.
EDI reduces the time spent processing transactions. The estimated per-claim savings of processing electronically instead of manually is $1 per claim for health plans, $1.49 for physicians, $.86 per claim for hospitals and $.83 per claim for others. When you process hundreds or thousands of claims, this adds up fast!

In addition, EDI reduces claims processing cycle times and provides online claims status reporting. EDI also saves on non-billing transactions; it reduces the waiting time for verification of eligibility and provides faster coordination between referring physicians.

**Privacy Standards Rule**

Now that the use of the Internet is commonplace, many people are concerned about how their personal information is used and distributed. No one wants his e-mail purchases, credit history or even supermarket choices accessible to any Tom, Dick or Mary with a modem. Certainly, most people have an even stronger interest in ensuring that their health information remains private.

The **Privacy Standards Rule** regulates the use and disclosure of individually identifiable health information. It defines the type of information covered and establishes patients’ rights of access to their own information. The intent of this rule is to allow patient information to be used and shared easily for treatment, healthcare operations and payment while at the same time safeguarding it from other, unauthorized uses.

The Privacy Standards Rule is really quite simple. It has two basic components:

- Limits on the use and disclosure of patients’ health information
- Patient rights regarding their health information

The Privacy Standards Rule allows for flexibility in implementing its guidelines. It often defers to the provider’s judgment. An understanding that patient care is the top priority drives the regulations, and impediments to quick, quality care have been avoided.

**Privacy and Business Associates**

The Privacy Standards Rule lets healthcare organizations enter this technological era with guarantees to their patients that health information will be protected. And the protection does not stop at covered entities. As of February 2010, the Privacy Standards Rule also applies to business associates. Remember, business associates are not employees of covered entities, but they use protected health information to perform a service for the entity. Some tasks business associates might perform include:

- Management of benefits, practices, quality assurance
- Data processing, such as transcription, coding and release of information
- Financial services, such as billing, claims processing/administration and
Consulting services, such as legal, actuarial, data aggregation, accreditation and utilization review

A sample Business Associate Agreement is attached at the end of this supplement for your review.

**Terminology of the Privacy Standards Rule**

The underlying premise of the Privacy Standards Rule is that information will stay private both within the healthcare industry and outside of it. To make the guidelines clear, HIPAA developed some very specific definitions.

**Protected Health Information (PHI)**

Protected Health Information (PHI) is individually identifiable health information (information that can be used to identify an individual) that is maintained or transmitted in any form, whether oral, written or electronic. (A few exceptions to the definition of PHI exist; these involve individually identifiable health information included in the educational records that the Family Educational Rights and Privacy Act (FERPA) covers.) This means that if you are a covered entity, you must be careful to protect all PHI. It is important to keep this fact in mind because the other three HIPAA rules cover only information that is maintained or transmitted electronically.

**Disclosure**

Disclosure is the release, transfer or provision of access to information outside the covered entity that holds information. The Privacy Standards Rule protects any means of divulging information, including oral, written and electronic communications.

**Use**

Use, on the other hand, refers to the sharing of protected health information within the entity that holds the information.

**Treatment, Payment and Health Care Operations (TPO)**

Under HIPAA, TPO stands for treatment, payment and health care operations. These letters appear often in the privacy regulations because they are at the heart of health care.

**Consent**

Many providers routinely have patients sign consent forms during the first visit. Consent means permission. These forms generally allow providers to use and disclose protected health information for TPO purposes.

**Authorization**

Authorizations are required for one-time disclosures outside the realm of TPO, such as releasing names to marketing firms, allowing medical information to be used for research and collecting information for a life insurance application.
The patient must sign authorizations. Authorizations generally have clear details about the intended use of the information, have expiration dates and specify and limit the type of information that can be released.

**Minimum Necessary**
The minimum necessary principle states that protected health information should be used or disclosed only to the extent needed to support the purpose of the use of disclosure. For example, staff at the information desk at a hospital do not need and should not have access to the entire file of a patient; instead, such workers need only the names, room and telephone numbers and, perhaps, status of the patient. The minimum necessary principle would thus limit the information accessible at the information desk to those items.

The healthcare professional has latitude in determining the practices and guidelines needed to meet this requirement. Since patient treatment must have the highest priority in the healthcare community, uses and disclosures made for treatment purposes are exempt from this requirement.

**Patient Rights**
Health records are much like property that someone else holds in trust. They are like having a safe deposit box at the bank. You can look at what’s there when you want, you control who else looks at the contents and you can add or remove items within reason. But since the safe deposit box is held at the bank, you must abide by some rules (such as hours of operation and size limitations) to keep your property there. In exchange for following the rules, you have the security of knowing that what’s held at the bank is safe and protected.

The HIPAA Privacy Standards Rule gives patients more control of their health information. A patient has several rights when it comes to his health record. He can:

- View it and request copies
- Control use and disclosure outside of TPO through authorizations
- Request a list of who else has accessed the record
- Request amendments to the record

The Privacy Standards Rule not only guarantees a patient certain rights regarding his health information, it also requires that the patient be informed of those rights and how they will be implemented and protected. Under the rule, providers and health plans must post a Notice of Privacy Practices and make a “good faith effort” to have patients read and sign the notice at the first visit. This notice lists the types of uses and disclosures of health information that are legally permitted or required without authorization from the patient. It also lets the patient know about his right to restrict certain aspects of these uses and disclosures. Patients have the right to examine and obtain a copy of their own health records and request corrections.
The Notice of Privacy Practices ensures that the patient is an informed participant in decisions that regard the sharing of his health information. It is a crucial element of the Privacy Standards Rule.

**Security and Electronic Signature Standards Rule**

Healthcare records are among the most valuable records in our society. They contain intensely private information, information that can be misused and create serious consequences if it falls into the wrong hands. Rejected loan applications, unfair or inappropriate employment decisions and embarrassing public exposure of personal information are all possible outcomes when healthcare records are misused.

For these reasons, healthcare information that is created, sorted or transmitted electronically needs strong protection. Computer hackers and viruses can wreak havoc on computer systems. They can corrupt files; make information public or sell it to financial, employment or media organizations; and change critical data. HIPAA’s security standards legislation aims to prevent such crimes.

The **Security and Electronic Signature Standards Rule**—effective April 20, 2005—spells out measures and methods to safeguard health information privacy and to keep the information secure. Under this rule, all health information—not just protected health information—that is electronically transmitted or maintained must be kept secure. HIPAA requires each covered entity to assess its own security needs and implement the measures that best meet those needs. Administrative, physical and technical concerns must be examined when these entities protect privacy. This doesn’t mean that every employee must now have top-secret clearance. Some changes can be simple. For
example, a good security step is to ensure that unauthorized people cannot view computer monitors and faxed pages. Other security measures are more complicated, such as using proper electronic data encryption.

HIPAA sets three basic requirements that cover security standards. Security standards must be:

- **Comprehensive**, addressing all aspects of security
- **Technologically neutral**, so each organization can incorporate the standards into its unique technical environment
- **Scalable**, so the security standards meet healthcare organizations of every size

Each organization must produce the required results. But how it does so is flexible. For example, all healthcare organizations must control access to their files. A small physician’s office might simply provide passwords for its personnel to meet this requirement. The office manager could access scheduling and billing information with her password, while the family nurse practitioner could renew prescriptions, view and modify health histories and review other, more confidential files with her password.

In a large hospital, the access requirements would be met with a much more complex set of tools. Key cards, PINs or tokens might be used for personnel to access particular rooms that house information databases within the multi-building complex. A security officer might view daily printouts that detail who accessed certain files with their passwords. She also might require password changes every few months.

The scalable feature of the security standards exists to ensure that compliance is economically feasible for organizations of every shape and size.

**Chain of Trust Agreements**

Under the proposed security regulations, covered entities are required to enter into Chain of Trust Agreements with their business associates. These agreements ensure that a uniform level of security is applied at every link of the chain as data passes from one entity to another. It would be virtually impossible for a covered entity to verify the security used before and after each transmission of data to and from its business associates. The Chain of Trust Agreement takes the place of such “in person” verification.

**Standard Identifiers Rule**

HIPAA sets standards for unique identifiers for three entities: providers, health plans and employers. Identifiers are unique numbers assigned to each business that help transfer information. The provider ID is the National Provider Identifier (NPI). The employer ID is the Employer Identification Number (EIN). The health plan ID uniquely identifies all organizations that pay for healthcare services. It’s also known as the National Payer ID. The use of standard identifiers is expected to ease the administrative challenges associated with all aspects of patient healthcare records. This includes documentation,
maintenance and billing requirements. These standard identifiers will allow the various entities within the healthcare system to most effectively and efficiently perform their respective financial, clinical, preventive and research functions. To put it simply, with the Standard Identifiers Rule, a healthcare entity can devote more time to its own particular business and less to general paper pushing.

**The Benefits of HIPAA and HITECH**

It costs the healthcare industry a lot of time and effort, as well as millions of dollars, to implement HIPAA regulations. Is it worth it? Consider this: For the first time in history, providers, payers and clearinghouses will use the same information in the same format. The improvement in communication is expected to cut overhead and administrative costs for everyone involved. The time and cost savings involved should help convince providers who don't already use electronic transactions to do so. Plus, the regulated protection will keep health information more private and secure.

**Financial Benefits**

The monetary benefits of HIPAA’s various electronic standards will begin almost immediately. However, because of the costs of compliance, these benefits most likely will not be apparent for a few years after implementation. Estimated savings to the industry as a whole are almost $30 billion from 2002 through 2011. These savings should affect all involved.

**Increased Consumer Confidence**

Americans are justifiably concerned about the way their confidential health information is used. HIPAA’s privacy and security regulations will ensure that a patient’s personal information is handled appropriately.

**Improved Health Claims Handling**

As was previously indicated, HIPAA will increase efficiency in handling claims. One major goal of HIPAA is to reduce the percentage of the healthcare dollars spent on administrative overhead with standardized formats and ID numbers, efficiency in handling claims processing and, consequently, more timely payments. Communications between providers, such as referrals, also will improve. The result will be lower administrative overhead expense and thus a greater percentage of the healthcare dollar spent on actual care.

**Penalties for Noncompliance**

HIPAA incorporates some strict penalties for noncompliance, abuse and fraud. The most severe penalties—including imprisonment—are levied for violations of a patient’s privacy. This indicates just how serious the public is about safeguarding confidential information. There are two types of penalties for ignoring the Privacy Standards Rule:

**Civil penalties:**
Offenders are fined $100 per offense with a maximum of $25,000 per person, per year for each requirement.

**Criminal penalties:**

- Obtaining or disclosing protected health information illegally could result in fines up to $50,000 and as much as a year in prison.
- Using false pretenses to obtain protected health information could result in fines up to $100,000 and up to five years in prison.
- Committing an offense with the intent to sell, transfer or use protected information could result in fines up to $250,000 and up to 10 years in prison.

**HIPAA and Your Job**

The HIPAA legislation is wide-reaching and often complex. Don’t allow all the requirements and rules to overwhelm you. To learn more, use the Internet to access the links provided in the next section. If you are an employee, talk to your employer about HIPAA and what it means for you. If you are self-employed, talk with your business associates and customers about HIPAA. Remember, HIPAA is designed to save you money and time and make everyone’s life easier in the long run!

**Further Information**

For more information about HIPAA, check out these Web sites. Remember that Web addresses change often.

**Phoenix Health Systems**

Phoenix Health Systems has set up this comprehensive and well-organized Web site about HIPAA, with links to the regulations themselves. You can also find up-to-date news articles and commentaries.
www.hipaadvisor.com

**American Health Information Management Association (AHIMA)**

The AHIMA Web site has a tremendous amount of information (including a number of HIPAA-related journal articles, checklists and the like) about HIPAA regulations.
www.ahima.org

**Centers for Medicare & Medicaid Services (CMS)**

CMS is the U.S. government agency that administers Medicare, Medicaid and the State Children’s Health Insurance Program (CHIP). There is also information specifically about HIPAA, including the complete text of the regulations and other important links.
www.cms.gov
www.cms.gov/hipaa

**Important Notice**
The Business Associate Agreement that follows is a sample agreement only. Furthermore, as of February 2010, such agreements must incorporate the additional requirements of ARRA/HITECH. Legal counsel must review all agreements to determine compliance with any applicable state and other law.

Also note that, most likely, this agreement would be appended to a Services Contract. The contract would spell out in detail the services the business associate provides to the covered entity and would contain other necessary provisions that the law requires.

**SAMPLE BUSINESS ASSOCIATE AGREEMENT**

THIS BUSINESS ASSOCIATE AGREEMENT (“Agreement”) is entered into on this ____ day of _____________, 20__ (the “Effective Date”), between [your provider office] ("Covered Entity") and _____________________ ("Business Associate") (each a “Party” and collectively the “Parties”).

WHEREAS, Covered Entity will disclose and/or make available to Business Associate Protected Health Information (“PHI”) in connection with services provided to Covered Entity by Business Associate, which information is confidential and must be given special protection; and

WHEREAS, Business Associate will have access to and/or create on behalf of and/or receive from Covered Entity Protected Health Information that can be used or disclosed only in accordance with this Agreement and the HHS Privacy Standards Rule;

NOW, THEREFORE, the Parties hereby agree as follows:

1. **DEFINITIONS.**

1.1 Disclosure. Disclosure shall mean the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

1.2 Health Care Operations. Health Care Operations shall have the meaning as set out in its definition in 45 CFR § 164.501, as such provision is currently drafted and as it is subsequently updated, amended, or revised.

1.3 HHS. HHS shall mean the Department of Health and Human Services.

1.4 HHS Privacy Standards Rule. HHS Privacy Standards Rule shall mean the Code of Federal Regulations (“CFR”), Title 45, §§ 160 and 164, as such regulations are currently drafted and as they are subsequently updated, amended, or revised.

1.5 Individual. Individual shall mean the person who is the subject of the Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

1.6 Protected Health Information. Protected Health Information shall have the meaning as set out in its definition in 45 CFR §164.501, as such provision is currently drafted and as it is subsequently updated, amended, or revised.

1.7 Secretary. Secretary shall mean the Secretary of Health and Human Services or
his/her designated representatives.

1.8 Use. Use shall mean, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

2. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION.

[2.1 Permitted Uses and Disclosures. The Parties hereby agree that, except as otherwise specified herein, Business Associate may make any and all uses and disclosures of PHI received from, created on behalf of, and/or made available by Covered Entity for the following stated purposes:

Here list the purposes for which PHI will be used, such as: to file health care claims on behalf of Covered Entity; to properly track the status of such claims; and to generate any necessary documentation for the above.] or, if a separate services contract is in place,

[2.1 Permitted Uses and Disclosures. The Parties hereby agree that, except as otherwise specified herein, Business Associate may make any and all uses and disclosures of PHI necessary to perform its obligations under the [name of services agreement].]

3. USE AND DISCLOSURE OF PHI FOR MANAGEMENT, ADMINISTRATION, AND LEGAL RESPONSIBILITIES.

3.1 Use. Notwithstanding the provisions of Section 2 above, Business Associate is permitted to use the PHI in its possession if necessary for its proper management and administration or to fulfill any present or future legal responsibilities of the Business Associate, provided that such uses are permitted under applicable Federal and State confidentiality laws.

3.2 Disclosure. Notwithstanding the provisions of Section 2 above, Business Associate is permitted to disclose the PHI in its possession to third parties if necessary for its proper management and administration or to fulfill any present or future legal responsibilities of the Business Associate, provided that the Business Associate represents to the Covered Entity in writing that (a) the disclosures are required by law, as provided for in 45 CFR § 164.501 or (b) the Business Associate has received from the third party written assurances regarding its confidential handling of such PHI as required under 45 CFR § 164.504(e)(4).

4. OTHER PERMITTED USES AND DISCLOSURES.

4.1 Data Aggregation Services. Notwithstanding the provisions of Section 2 above, Business Associate is permitted to use and/or disclose PHI to provide data aggregation services, as that term is defined in 45 CFR § 164.501, relating to the Health Care Operations of Covered Entity.

5. RESPONSIBILITIES OF BUSINESS ASSOCIATE WITH RESPECT TO PHI.

5.1 Limits on Use and Disclosure. Business Associate hereby agrees that PHI created on behalf of or provided or made available by Covered Entity shall not be further used or
disclosed by Business Associate other than as permitted or required by this Agreement or as otherwise required by law. Except as permitted in Sections 3 and 4 above, Business Associate shall not use or further disclose PHI in a manner that would violate the requirement of the HHS Privacy Standards Rule if done by Covered Entity.

5.2 Reports of Improper Use or Disclosure. Business Associate hereby agrees to report to Covered Entity any use and/or disclosure of PHI that is not permitted or required by this Agreement of which Business Associate becomes aware within ___ days of Business Associate’s discovery of such unauthorized use and/or disclosure.

5.3 Appropriate Safeguards. Business Associate will establish and maintain appropriate safeguards to maintain the security of PHI and to prevent any use or disclosure of such PHI other than as provided for by this Agreement.

5.4 Subcontractors and Agents. Business Associate hereby agrees that whenever PHI is provided or made available to any of its subcontractors or agents as permitted by this Agreement, Business Associate will require such subcontractors or agents to agree, in writing, to adhere to the same terms, conditions, and restrictions on the use and/or disclosure of PHI that apply to Business Associate pursuant to this Agreement.

5.5 Right of Access of an Individual. At the request of and in the time and manner designated by Covered Entity, Business Associate hereby agrees to make available and provide a right of access to PHI by Covered Entity or the Individual, in accordance with the provisions of 45 CFR § 164.524.

5.6 Amendments to PHI. At the request of and in the time and manner designated by Covered Entity, Business Associate hereby agrees to make PHI available for amendment and to incorporate any amendment(s) to PHI pursuant to 45 CFR § 164.526.

5.7 Accounting of Disclosures. (a) Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.508. (b) Within 45 days of receiving a written request from Covered Entity, Business Associate hereby agrees to make such information available to Covered Entity as is requested by Covered Entity to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR § 164.528.

5.8 Access to Books and Records. Business Associate shall make available to the Secretary its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity for the purposes of determining Covered Entity’s compliance with the Privacy Rule, in accordance with 45 CFR § 164.504(e)(2)(ii)(H).

6. RESPONSIBILITIES OF COVERED ENTITY WITH RESPECT TO PHI.

6.1 Change in Notice of Privacy Practices. Covered Entity agrees to inform Business Associate of any changes in the form of the Notice of Privacy Practices that Covered Entity provides to Individuals pursuant to 45 CFR § 164.520, and agrees to provide Business
6.2 Change or Withdrawal of Permission. Covered Entity agrees to inform Business Associate of any changes in the form of, or revocation of, permission by an Individual to use or disclose PHI, to the extent such changes may affect Business Associate’s use or disclosure of PHI.

6.3 Changes in Requirements. Covered Entity agrees to notify Business Associate of any arrangements permitted or required of Covered Entity under the HHS Privacy Standards Rule that may impact in any manner the use and/or disclosure of PHI by the Business Associate under this Agreement, including, but not limited to, restrictions on use and/or disclosure of PHI as provided for in 45 CFR § 164.522 agreed to by Covered Entity.

6.4 Permissible Requests. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HHS Privacy Standards Rule if done by Covered Entity, except as provided in Sections 3 and 4 above.

7. TERM AND TERMINATION.

7.1 Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the Parties have been met, unless terminated as provided in this section.

7.2 Termination of Agreement. Pursuant to 45 CFR § 164.504(e)(2)(iii), Business Associate agrees Covered Entity may immediately terminate this Agreement if Covered Entity determines that Business Associate has violated a material term of this Agreement. Alternatively, Covered Entity may choose to (a) provide Business Associate with __ days’ written notice of the existence of an alleged material violation, and (b) afford the Business Associate an opportunity to cure said alleged material violation upon mutually agreeable terms. If mutually agreeable terms cannot be reached within __ days, then Business Associate must cure said violation within __ days to the satisfaction of Covered Entity. If Business Associate fails to cure such violation as set forth in this paragraph, Covered Entity may immediately terminate this Agreement. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

7.3 Effect of Termination. Upon the termination of this Agreement, Business Associate agrees to return or destroy all PHI received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate or its subcontractors or agents still maintain in any form, pursuant to 45 CFR § 164.504(e)(2)(ii)(I). Business Associate agrees that it shall not retain any copies of such PHI. Alternatively, if such return or destruction of such PHI is not feasible, then Business Associate agrees to extend the protections of this Agreement to such PHI for as long as necessary and to limit further uses and disclosures to those purposes that make the return or destruction of such PHI infeasible.

8. MISCELLANEOUS.

8.1 Governing Law. This Agreement shall be governed by the laws of the State of ______________________.
8.2 Notice. Whenever under this Agreement one Party is required to give notice to the other, such notice shall be deemed given if mailed by First Class United States mail or by express courier, postage prepaid, to such Party’s address as given below, and/or via facsimile to the facsimile telephone numbers listed below.

<table>
<thead>
<tr>
<th>Business Associate</th>
<th>Covered Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Attention:</td>
<td>Attention:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Fax:</td>
<td>Fax:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each Party may at any time change its address and that of its representative for notice by giving notice thereof in the manner provided above.

8.3 Headings. The headings of this Agreement are included for ease of reference only and shall not enter into the interpretation of this Agreement.

8.4 Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed to be an original. Facsimile copies of this Agreement shall be deemed to be originals.

**IN WITNESS WHEREOF**, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf effective as of ________________, 20__.  

**BUSINESS ASSOCIATE**

<table>
<thead>
<tr>
<th>By:</th>
<th>By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print name:</td>
<td>Print name:</td>
</tr>
<tr>
<td>Print title:</td>
<td>Print title:</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>

**COVERED ENTITY**
<table>
<thead>
<tr>
<th>Glossary Entry</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Simplification</td>
<td>Title II, Subtitle F of HIPAA that sets up nationally consistent regulations in four main areas: electronic transactions, privacy, security and identification numbers.</td>
</tr>
<tr>
<td>Chain of Trust Agreements</td>
<td>Agreements that ensure that a uniform level of security is applied at every link of the chain as data passes from one entity to another.</td>
</tr>
<tr>
<td>Covered entities</td>
<td>Providers that transmit health information electronically, such as health plans and healthcare clearinghouses.</td>
</tr>
<tr>
<td>Electronic</td>
<td>A transaction that is transmitted with an electronic medium.</td>
</tr>
<tr>
<td>Electronic Transaction Standards Rule</td>
<td>A rule that set both the formats for and the specific codes to be used in insurance claims.</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>A bill that Congress enacted in 1996. It has two main objectives. The first objective (portability) is to ensure the continuation of health insurance coverage for workers and their families during times of job change or loss. The second (accountability) is to increase the effectiveness of the healthcare system while protecting health data integrity, confidentiality and availability and preventing fraud and abuse.</td>
</tr>
<tr>
<td>HIPAA (Health Insurance Portability and Accountability Act)</td>
<td>A bill that Congress enacted in 1996. It has two main objectives. The first objective (portability) is to ensure the continuation of health insurance coverage for workers and their families during times of job change or loss. The second (accountability) is to increase the effectiveness of the healthcare system while protecting health data integrity, confidentiality and availability and preventing fraud and abuse.</td>
</tr>
<tr>
<td>Identifiers</td>
<td>Unique numbers assigned to each business that help transfer information.</td>
</tr>
<tr>
<td>Privacy Standards Rule</td>
<td>A rule that regulates the use and disclosure of individually identifiable health information.</td>
</tr>
<tr>
<td>Security and Electronic Signature Standards Rule</td>
<td>A rule that became effective April 20, 2005. It spells out measures and methods used to safeguard health information privacy and to keep the information secure.</td>
</tr>
<tr>
<td>Titles</td>
<td>The different sections of HIPAA.</td>
</tr>
<tr>
<td>Transaction</td>
<td>The transmission of information between two parties to carry out the financial or administrative activities that occur in a medical facility or office other than those related to treatment.</td>
</tr>
</tbody>
</table>
Table of Contents

HIPAA and You 5
What Is HIPAA? 5
  The HITECH Act 6
Administrative Simplification 6
  Covered Entities 7
Electronic Transaction Standards Rule 7
  How Does HIPAA Define Electronic? 8
  What Is a Transaction? 8
  The Benefits of Using Electronic Transaction Standards 9
Privacy Standards Rule 10
  Privacy and Business Associates 10
  Terminology of the Privacy Standards Rule 11
  Patient Rights 12
Security and Electronic Signature Standards Rule 13
  Chain of Trust Agreements 14
Standard Identifiers Rule 14
The Benefits of HIPAA and HITECH 15
  Financial Benefits 15
  Increased Consumer Confidence 15
  Improved Health Claims Handling 15
  Penalties for Noncompliance 15
HIPAA and Your Job 16
Further Information 16
Glossary 22