



HIPAA Overview

Background:

“HIPAA” is an acronym, which stands for the Health Insurance Portability and Accountability Act of 1996. HIPAA is a very complex federal law involving a myriad of federal regulations.

HIPAA is a term that many are familiar with, but few actually understand. This overview, while only scratching the surface of HIPAA, will hopefully assist in demystifying some of the more relevant portions of HIPAA for our payers, providers, and members. The text that follows is only meant to supplement and guide you to the links provided. The links will guide you to information provided directly to the public by the Department of Health and Human Services or other entity.

It is important to note that this overview is not legal advice. This information is only provided as general educational material. Any issues you may encounter with this law or its accompanying regulations should be discussed with competent counsel.

For HIPAA compliance dates, please click on the following link:

<http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAAComplianceDeadlines.pdf>

Covered Entities:

A Covered Entity is defined in the regulations as:

- a health plan,
- a health care clearinghouse, or
- a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

Covered Entities are the only entities that are directly subject to the provisions of HIPAA. Determining whether or not your entity is a Covered Entity can sometimes be tricky. The assistance of legal counsel is suggested. The Department of Health and Human Services Centers for Medicare and Medicaid Services (“CMS”) has also provided an online tool to assist in making this determination.

<http://www.cms.hhs.gov/apps/hipaa2decisionsupport/default.asp>

Covered Entities are directly governed by the terms of the law and regulations and must abide by the requirements set forth therein. Other entities are not directly subject to the terms of HIPAA, but may be subject to these same provisions through contracts known as Business Associate Agreements or subcontractor agreements.

Business Associates and Business Associate Agreements:

The definition of a Business Associate is not as clear as that of a Covered Entity. Generally speaking, a Business Associate is any person or entity that provides services to a Covered Entity, which either fall under the provisions of HIPAA or that involve the use or disclosure of individually identifiable health information. This would include the Covered Entity's service providers such as attorneys, accountants, billing companies, etc. It is also common to include such service providers as shredding and cleaning companies in this classification due to the fact that they may come into contact with individually identifiable health information.

The consequence of being a Business Associate is that the person or entity is contractually required to abide by the terms of HIPAA through the execution of a Business Associate Agreement. This Business Associate Agreement is a contract that binds the Business Associate to agree to abide by the terms of HIPAA. The Covered Entity generally provides the Business Associate Agreement to the Business Associate, as it is the Covered Entity's responsibility to have this agreement in place prior to allowing work to be performed on its behalf. The material terms of the Business Associate Agreement are derived directly from the regulations.

Health and Human Services Office of Civil Rights ("OCR") has provided a sample version of language that may be used in a Business Associate Agreement. This language of course, is only provided as a guide or a starting point, but is an excellent resource. The actual terms of the Agreement should be carefully reviewed with legal counsel and negotiated according to the terms of the situation at hand. To view this sample language, you may click on the link below.

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/contractprov.html>

Privacy Rule:

Generally speaking, the HIPAA Privacy Rule is designed to safeguard patient information (also known as protected health information or PHI) from any unauthorized use or disclosure. The Department of Health and Human Services has provided a great overview of the Privacy Rule. That overview document can be viewed by clicking on the following link:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/>

Clicking on the following link will provide you with an additional summary resource:

<http://www.hhs.gov/news/facts/privacy.html>

Links to the actual privacy regulations can also be found on the HHS site. Please click on the link below to view this information.

<http://www.hhs.gov/ocr/privacy/hipaa/faq/about/>

The Privacy Rule was designed to protect the privacy of patient information and clarify the roles and responsibilities in regards to the handling and treatment of this information. Individually identifiable health information, PHI, or protected individually identifiable

health information is any information pertaining to a patient that in any way relates to or identifies that patient. The actual definitions contained within the regulations are considerably longer. Any question as to whether or not some amount of information is protected under HIPAA should be resolved by analyzing the data against the regulations.

The Privacy Rule contains various restrictions on how and when this information may be disclosed, used, or accessed and by whom. The Privacy Rule also specifies what records must be kept when that information is wrongly disclosed.

Security Rule:

The Security Rule is a group of regulations whose primary goal is to ensure the security and integrity of individually identifiable health information that is stored or transmitted in electronic format. The Security Rule includes a variety of specific requirements that must be implemented by Covered Entities. These requirements fall within three categories:

- Administrative security,
- Technical security, and
- Physical security.

Unlike the Privacy Rule, not all aspects of the Security Rule are absolutely mandatory. However, it is important to note that the Security Rule portions that are not mandatory (designated as addressable) must be thoroughly evaluated and analyzed prior to carefully documenting why the particular standard was not implemented. A Covered Entity may only choose to not implement an addressable standard if it clearly cannot do so and can document why that it is unable to do so.

CMS provides a link to the final Rule. That link is:

<http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>

The document above can prove somewhat confusing. However, a helpful chart is provided on page 48 of the .pdf file, which can serve as an overview prior to reading the document. The chart can also help to serve as a guideline for implementing all of the requirements of the Security Rule.

Transactions and Code Sets Standards:

The Transactions and Code Sets Standards specify how electronic claims transactions are to be conducted. Covered Entities conducting electronic transactions must do them in accordance with such specifications. Health and Human Services provides a link to the final rule. That link is directly below:

<http://www.cms.hhs.gov/TransactionCodeSetsStandards/Downloads/txfinal.pdf>

The ANSI X12 Implementation Guides may be downloaded in .pdf format for free by clicking on the following link:

<http://www.wpc-edi.com/hipaa>

Summary:

The information provided on this page is simply a beginning to understanding various portions of HIPAA. This was not meant to be a comprehensive overview of the law, but a resource. To better understand the law and the regulations, it is imperative that one read the information on the linked pages and consult with legal counsel.

If there is a problem encountered in attempting to access some of the information above, [e-mail Midlands Choice Legal Counsel](#).