



Locum Employee HIPAA Privacy Rule & Security Rule Self Verification

OVERVIEW

This overview has been created to review the basic information concerning Healthcare Professionals and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This overview will help you become familiar with the basics of HIPAA. Please read it in its entirety and complete the HIPAA Self Verification Form at the end.

This is only a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. If you have any questions regarding HIPAA you should contact your facility's Privacy Officer.

What is HIPAA?

The U.S. Department of Health and Human Services ("HHS") issued the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

The overall goal of HIPAA is to provide insurance portability, fraud enforcement, and administrative simplification for the healthcare industry. HIPAA was formed, overall, to keep healthcare information private, to consolidate nonstandard healthcare data and transaction formats, to streamline healthcare operations, and to reduce the cost of providing healthcare services.

HIPAA Administrative Simplification

The Administrative Simplification section was designed to decrease the costs of healthcare administration with the goal of using that money to improve the quality of healthcare, standardizing electronic transactions, national identifiers, and to safeguard Protected Health Information (PHI). The Administrative Simplification includes mandates for the privacy and security of personal and confidential healthcare information, referred to as the Privacy Rule and the Security Rule.

The Privacy Rule

The Privacy Rule establishes national standards for the protection of certain health information. A major goal of the Privacy Rule is to assure that individuals' information is properly protected while allowing the flow of information needed to provide and promote high quality healthcare, and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the healthcare marketplace is diverse,



the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

The Privacy Rule standards address the use and disclosure of individuals' PHI by organizations subject to the Privacy Rule ("Covered Entities"), as well as standards for individuals' privacy rights to understand and control how their health information is used.

Who is covered by the Privacy Rule?

Organizations that must comply with HIPAA are called Covered Entities (CE). Covered entities are virtually the entire healthcare industry as well as a significant number of organizations in other industries. In other words any provider or organization who transmits and uses health information in any form or media, whether electronic, printed, or oral is a Covered Entity.

There are three main CE categories:

- Healthcare Provider: An individual, a group or an organization licensed or authorized to provide medical care, equipment, supplies, or professional services, including billing and payment.
- Health Plans: Individual or group plans that provide or pay for medical care.
- Healthcare clearinghouses: Public or private entities that convert elements of health information from non standard format to standard, or vice versa.

What information is protected?

The Privacy Rule protects all "Individually Identifiable Health Information" (IIHI) held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. The Privacy Rule calls this information "Protected Health Information" (PHI).

IIHI is information, including demographic data, that relates to:

- Individual's past, present or future physical or mental health or condition
- Provision of healthcare to the individual
- Past, present, or future payment for the provision of healthcare to the individual

IIHI includes many common identifiers (e.g., name, address, birth date, Social Security Number)

General Principle

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.



Authorized Uses and Disclosures

“Use” means the sharing, employment, application, utilization, examination, or analysis of IHI within a CE. “Disclosure” is the release, transfer, provision of access to, or divulging information outside the entity holding the information.

A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or healthcare operations or otherwise permitted or required by the Privacy Rule. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.

To view the entire Privacy Rule, and for other additional helpful information see the OCR website: <http://www.hhs.gov/ocr/hipaa>

Security Rule Overview

The Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule sets the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that Covered Entities must put in place to secure individuals’ “electronic protected health information” (e-PHI). The Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

A major goal of the Security Rule is to protect the privacy of individuals’ health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity’s particular size, organizational structure, and risks to consumers’ e-PHI.

General Rules

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.



Security Rule definitions:

- “Confidentiality” means that e-PHI is not available or disclosed to unauthorized persons. The Security Rule’s confidentiality requirements support the Privacy Rule’s prohibitions against improper uses and disclosures of PHI.
- “Integrity” means that e-PHI is not altered or destroyed in an unauthorized manner.
- “Availability” means that e-PHI is accessible and usable on demand by an authorized person.

Covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments.

When a covered entity is deciding which security measures to use, the Rule does not dictate those measures, but requires the covered entity to consider:

- Its size, complexity, and capabilities,
- Its technical, hardware, and software infrastructure,
- The costs of security measures, and
- The likelihood and possible impact of potential risks to e-PHI.

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.

For more information on the Security Rule visit

http://www.cms.gov/HIPAAGenInfo/04_PrivacyandSecurityStandards.asp#TopOfPage



**MISSION SEARCH
LOCUM EMPLOYEE HIPAA SELF VERIFICATION**

I, _____, hereby verify that I have read and understand the HIPAA Privacy Rule & Security Rule Overview. I verify that I understand my responsibilities and I understand that if I have any questions regarding HIPAA I should contact my facility's Privacy Officer.

Signature

Date

Printed Name