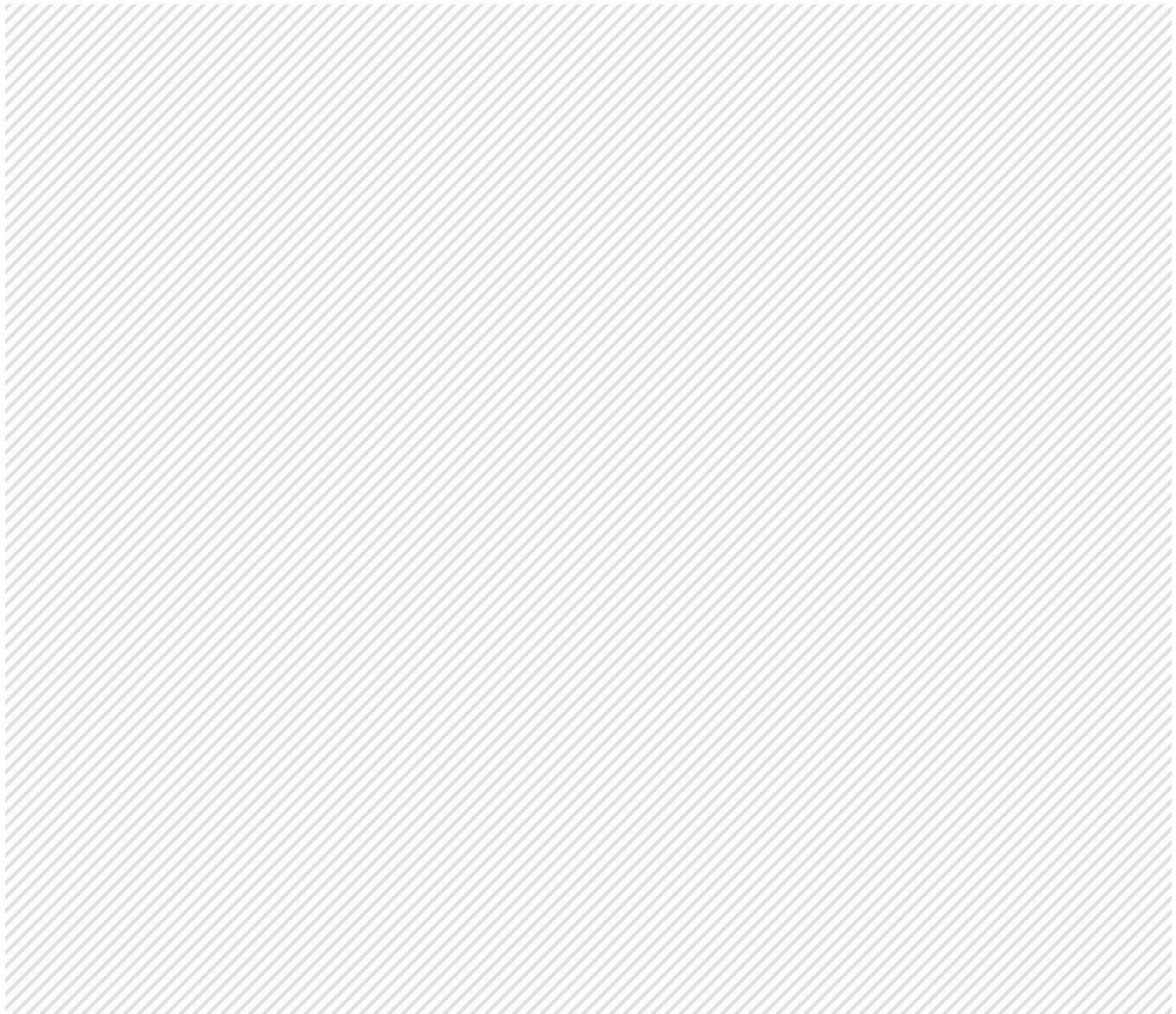


HIPAA

Core Competency Inservice

January 2020



This guide may not be reproduced, stored in a retrieval system, or transmitted, in any form, in whole or in part, or by any means, electronic, mechanical, recorded, or otherwise, without the prior written consent of HealthcareSource HR, Inc. The information in this guide is subject to change without notice. HealthcareSource HR, Inc. assumes no responsibility or liability for any errors, omissions, assumptions, or any conclusions drawn from this guide. All other third-party trademarks mentioned in this publication are the property of their respective owner.

Table of Contents

Introduction	3
Five HIPAA Rules.....	3
<i>Privacy Rule</i>	<i>3</i>
<i>Security Rule.....</i>	<i>3</i>
<i>Transaction and Code Sets Rule</i>	<i>4</i>
<i>Covered Transactions.....</i>	<i>4</i>
<i>Unique Identifier Rule.....</i>	<i>4</i>
<i>Enforcement Rule</i>	<i>5</i>
HITECH Act.....	5
Other Uses of Protected Health Information.....	5
<i>Marketing.....</i>	<i>5</i>
<i>Incidental Disclosures.....</i>	<i>5</i>
<i>Patients Rights</i>	<i>5</i>
References.....	6

Introduction

HIPAA, which stands for the American Health Insurance Portability and Accountability Act, is a set of rules set forth to regulate and improve healthcare insurance, fraud and abuse. HIPAA also ensures that every healthcare entity protects patient information. Every healthcare entity is required to create patient privacy policies and procedures that reflect the strict rules that HIPAA has set forth.

HIPAA regulations impact virtually every department of every healthcare entity that has access to confidential healthcare information. These include, but are not limited to, hospital/LTAC/SNF/home health staff (physicians, nurses, social workers, physical therapists, respiratory therapists, occupational therapists, secretaries, billing staff, medical transcriptionists, lab technicians, and radiology technicians involved in the patient's care), private medical practices, free healthcare clinics/community health, billing firms, auditors, lawyers, consultants, insurance companies, medical clearing houses, Medicare, Medicaid, medical device manufacturers, and other healthcare organizations.

Five HIPAA Rules

Privacy Rule

HIPAA created nationwide Privacy Rules to ensure the protection of patients' healthcare information. A patient's private healthcare information would include, but is not limited to, the medical record (health history, diagnosis, and plan of care), personal information (address and social security number), and healthcare payment method (insurance information, Medicare/Medicaid, and credit card/bank account information). The Privacy Rule must be followed by any person dealing with patients' paper or electronic healthcare information.

The HIPAA Privacy Rule created regulations to protect the privacy of personal health information, as well as limit the people who have access to private healthcare information. Only those directly involved in a patient's care, billing, or payment have legal access to his or her healthcare information. Each person involved in the case only has legal access to information needed to complete their job correctly.

The Privacy Rule ensures that patients have certain rights when it comes to their healthcare information. All patients have the right to read their medical record, to correct any false information on their medical record, and to have a copy of their personal health records in their possession if they so choose.

Despite the privacy rule, HIPAA cannot protect all personal healthcare information from the Center for Disease Control (CDC). By law every healthcare provider must report infectious diseases, such as HIV, Hepatitis A, and Tuberculosis, to the Center for Disease Control (CDC).

Security Rule

The HIPAA Security Rule is designed to protect all electronic healthcare information. The Security Rule helps define policies and procedures that protect all electronic healthcare information by regulating how information is accessed, who is allowed to access the information, how the information is saved, how the information is safely transmitted, and how to safely and effectively audit the system.

The HIPAA Security Rule created three ways to improve the security of electronic healthcare information. These include, **Technical Safeguards** (which limit computer access to healthcare information through the use of passwords and encryptions), **Physical Safeguards** (which limit access to facility computers by keeping them physically out of reach of people who are not granted access), and **Administrative Safeguards** (which develop a security team and officer to update, enforce, and monitor the HIPAA security plan and complete HIPAA risk analysis).

Transaction and Code Sets Rule

To ensure information remains private, HIPAA requires a Code Set to be used to encode healthcare data such as medical terms, medications, clinical manifestations, what caused the illness or injury, care plan, prevention methods, medical concepts, medical diagnosis, medical equipment/supplies used for treatment, and medical procedure codes.

Covered Transactions

The transaction standards for electronic healthcare enable healthcare providers and insurance companies to communicate more fluidly. The HIPAA transaction codes cover:

- Healthcare claims
- Health plan eligibility
- Enrollment and disenrollment in a health plan
- Healthcare payment
- Health plan premium payments
- Claims, inquiries, and responses
- Referral certification and authorization
- Benefits

Unique Identifier Rule

- The HIPAA Administrative Simplification regulation created three types of identifiers used to simplify and organize administrative and financial healthcare transactions. These identifiers include:
- Standard Unique Employer Identifier.
- This is the same unique number each employer uses on IRS forms to identify themselves. The same number is used for HIPAA identification.
- National Provider Identifier (NPI).
- The NPI is a unique number used to identify each healthcare provider.
- National Health Plan Identifier (NHI)
- The NHI identifies healthcare plans for payment and billing purposes.

Enforcement Rule

The enforcement rule helps establish HIPAA violations and creates criminal and civil penalties for those violations. The HITECH Act created the enforcement rule.

HITECH Act

The HITECH Act gives money, funded by Medicare and Medicaid, to facilities who acquire certain technology that will help improve patient care and help protect patient healthcare information, such as electronic health records (EHRs). The HITECH Act also sets guidelines for punishments for HIPAA violators, in any field of business, who are involved with patient healthcare information.

Other Uses of Protected Health Information

Marketing

A healthcare facility, or entity involved in healthcare information, may not use or disclose protected healthcare information for purposes other than treatment, payment, and healthcare operations, without the patient's written authorization.

Personal health information cannot be disclosed for marketing purposes without the patient's written authorization. For example, a pharmacist may not provide a pharmaceutical company a list of patients with a particular disease in order for the pharmaceutical company to sell drugs to those patients without their authorization.

Incidental Disclosures

The Privacy Rule allows "incidental" disclosures of personal health information, as long as the facility uses set safeguards and adheres to the "minimum necessary" standard. For example, doctors' offices may use waiting room sign-in sheets, and medical staff may confer at the nurse's station without violating the Privacy Rule.

Patients Rights

HIPAA's focus is on the Rights of the Patient and confidentiality of their information. Under HIPAA, patients have the right to several key issues: Right to Request Amendment of their medical record. Right to Request to Inspect and Copy their record. Right to Restrict what information and to whom it can be released to. Right to Receive Confidential Communication. Right to Complain about a disclosure of their PHI.

References

<http://www.cms.gov/Regulations-and-Guidance/HIPAA-AdministrativeSimplification/HIPAAGenInfo/index.html?redirect=/HIPAAgeninfo/>
<http://www.hhs.gov/ocr/hipaa> 2019

Center for Disease Control and Prevention. Summary of Notifiable Diseases --- United States, 2009. May 13, 2011, 58(53); 1-100. <http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5853a1.htm>

Health Information Privacy For Covered Entities and Business Associates, Accessed Nov 2014;
<http://www.hhs.gov/ocr/privacy/HIPAA/understanding/coveredentities/index.html>

HIPAA 101Guide to Compliance Rules & Laws. HIPAA Security Rule and Compliance. November 1, 2016.
<http://www.HIPAA-101.com/HIPAA-security.htm>

HIPAA 101Guide to Compliance Rules & Laws. HIPAA and the HITECH Act. November 17, 2016.
<http://www.HIPAA-101.com/HIPAA-hitech.htm>

HIPAA 101Guide to Compliance Rules & Laws. HIPAA Enforcement Rule and Compliance. November 17, 2016.
<http://www.HIPAA-101.com/HIPAA-enforcement.htm>

HIPAA 101Guide to Compliance Rules & Laws. Unique Identifiers Rule (Administrative Simplification). November 17, 2016. <http://www.HIPAA-101.com/HIPAA-identifiers.htm>

HIPAA 101Guide to Compliance Rules & Laws. HIPAA Transaction & Code Sets Rule. November 17, 2016.
<http://www.HIPAA-101.com/HIPAA-transaction.htm>

HIPAA 101Guide to Compliance Rules & Laws. HIPAA Privacy Rule and Compliance. November 17, 2016.
<http://www.HIPAA-101.com/HIPAA-privacy.htm>