
HIPAA
The Health Insurance Portability and Accountability Act of 1996

Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal law enacted in the United States to safeguard the privacy and security of individuals' protected health information (PHI). HIPAA consists of several regulations that govern how healthcare providers, health plans, and their business associates handle and protect PHI.

This law has 5 rules: Privacy Rule, Security Rule, Omnibus Rule, Breach Notification Rule, and Enforcement Rule.

LEGENDS

PHI - Protected Health Information
ePHI - Electronic Protected Health Information
HHS - Health and Human Services
OCR - Office of Civil Rights

COVERED ENTITIES

Dentists

Insurance Companies

Pharmacies

Optometrists

Doctors Offices

Covered Entities

A covered entity can be health care providers, health plans and health care clearinghouses involved in the transmission of protected health information (PHI)

Do I need to be HIPAA Compliant?

Anyone who handles PHI needs to be HIPAA compliant including but not limited to…

A business associate is any individual or entity that may encounter PHI through dealings with covered entities.

Business Associates

MSPs

Shredding Companies

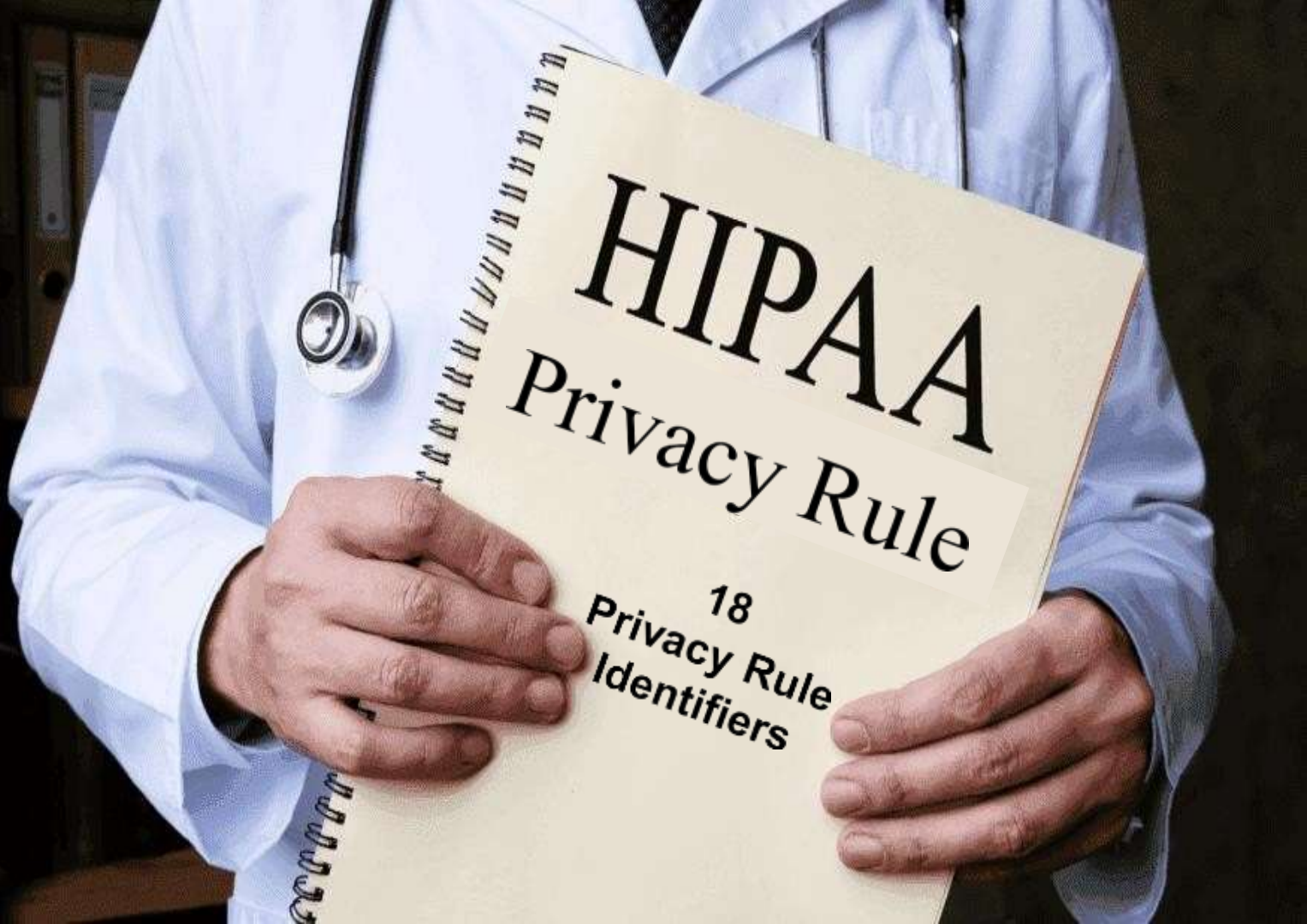
Lawyers

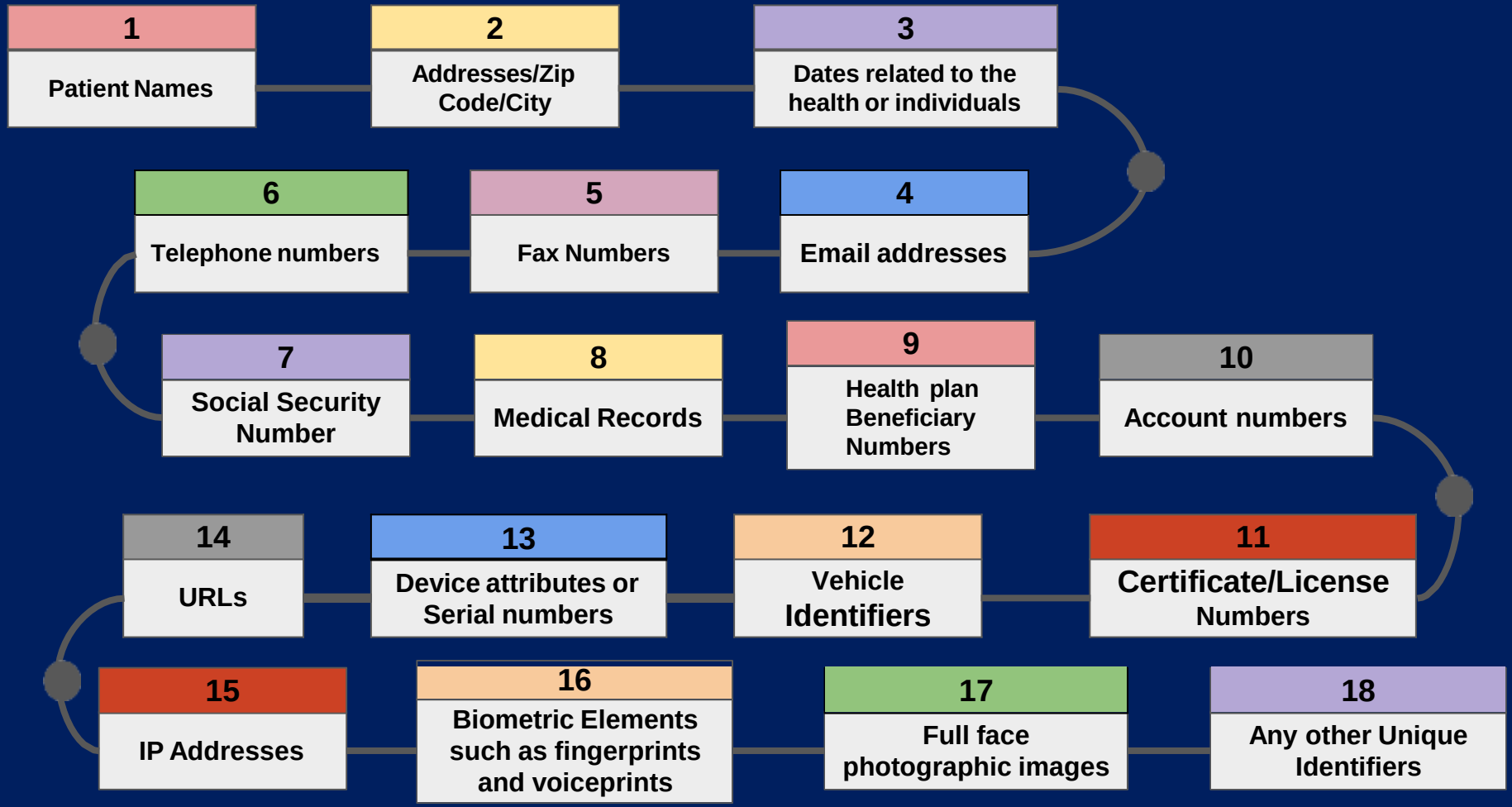
Answering Services

Billing Companies

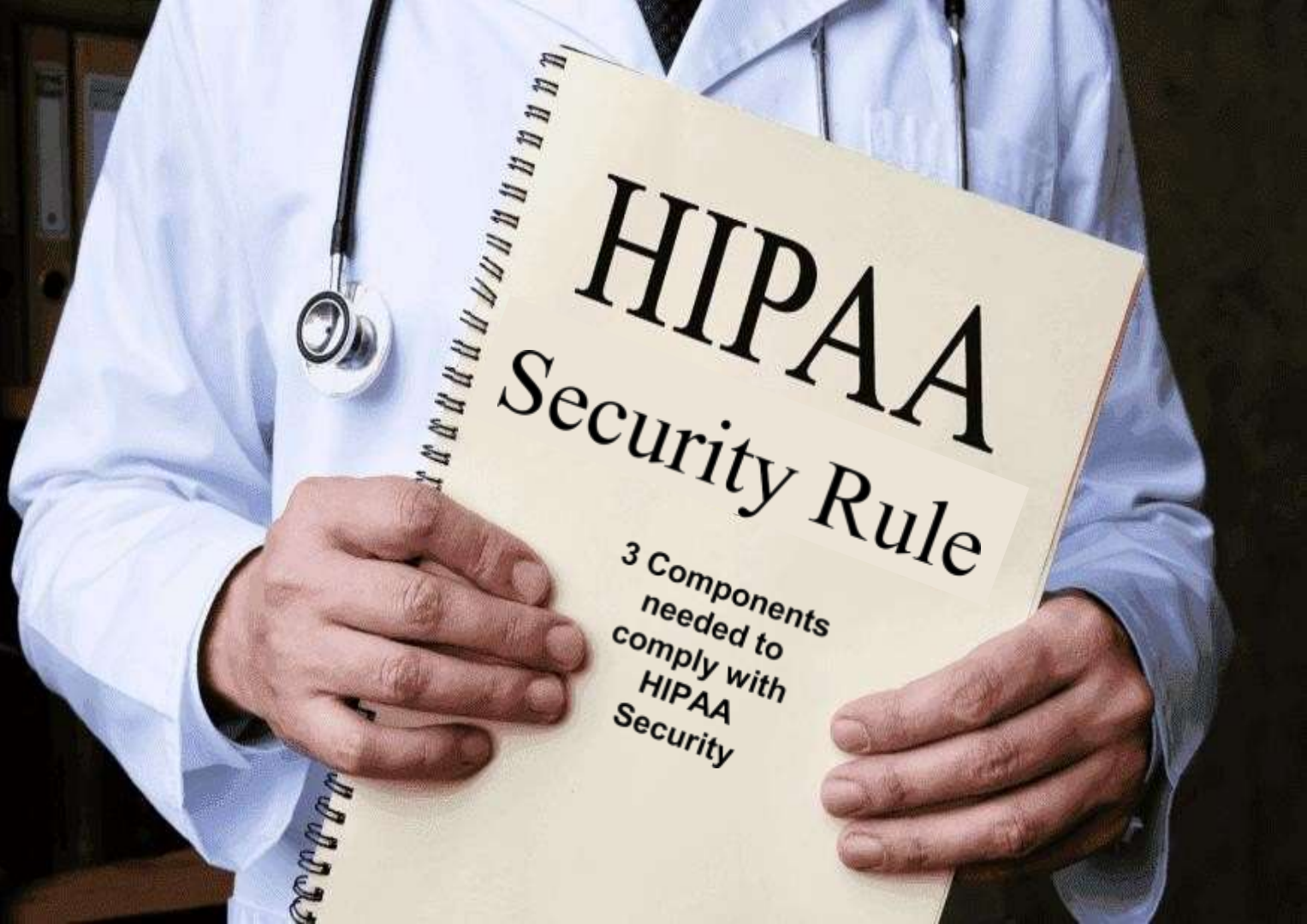
The Privacy Rule establishes the standards for protecting individuals' PHI by limiting its use and disclosure. It grants patients certain rights over their health information, including the right to access their own records, request corrections, and control how their information is shared.

The Privacy Rule includes a set of 18 identifiers. These identifiers are crucial to the enforcement of privacy protections under HIPAA, as they help define what constitutes PHI that requires special handling and protection.




1
Patient Names
2
Addresses/Zip Code/City
3
Dates related to the health or individuals
4
Email addresses
5
Fax Numbers
6
Telephone numbers
7
Social Security Number
8
Medical Records
9
Health plan Beneficiary Numbers
10
Account numbers
11
Certificate/License Numbers
12
Vehicle Identifiers
13
Device attributes or Serial numbers
14
URLs
15
IP Addresses
16
Biometric Elements such as fingerprints and voiceprints
17
Full face photographic images
18
Any other Unique Identifiers

The Security Rule sets forth security standards for electronic protected health information (ePHI). Covered entities are mandated to implement safeguards to ensure the confidentiality, integrity, and availability of ePHI. This includes implementing physical, technical, and administrative measures to protect against unauthorized access or breaches.



3 COMPONENTS OF HIPAA SECURITY RULE

ADMINISTRATIVE REQUIREMENTS

This rule establishes standards for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI). This rule applies to covered entities (healthcare providers, health plans, and healthcare clearinghouses) and their business associates. Here are some of the administrative requirements outlined in the HIPAA Security Rule:

- Assign a security official who is responsible for developing and implementing the organization's security policies and procedures.
- Identify which employees/individual have access to patient data/information.
- Must provide regular security training to their workforce to ensure that employees understand the importance of security and its policies.
- Require all outside parties who need to access protected patient data to sign contracts stating that they will comply with HIPAA security rules.
- Back-up data and have an emergency plan for disasters that could cause information loss.
- Perform an annual data security assessment.
- Create a data breach response plan that addresses notifying affected patients and fixing compromised IT systems.

3 COMPONENTS OF HIPAA SECURITY RULE

PHYSICAL SECURITY REQUIREMENTS

This rule includes physical security requirements to safeguard electronic protected health information (ePHI) and ensure the confidentiality, integrity, and availability of this sensitive data. Here are the key physical security requirements outlined in the HIPAA Security Rule:

Facility Access Controls - Implement policies and procedures to limit physical access to their facilities and electronic information systems that contain ePHI. (i.e using methods like facility security plans, access badges, electronic locks, and surveillance systems.)

Workstation and Device Security - Implement physical safeguards to restrict access to workstations and devices that can access ePHI. (i.e using screen locks, authentication mechanisms, and securing portable devices to prevent unauthorized access.)

HIPAA

Device and Media Controls - Policies and procedures must be in place to manage and control the movement of hardware and electronic media that contain ePHI. (i.e inventory management, data disposal procedures, and secure media disposal.)

Security Incident Response and Reporting - Implement procedures to respond to security incidents involving ePHI, including unauthorized access or breaches of physical security. (i.e reporting incidents, investigating the breach, and mitigating any potential harm.)

3 COMPONENTS OF HIPAA SECURITY RULE

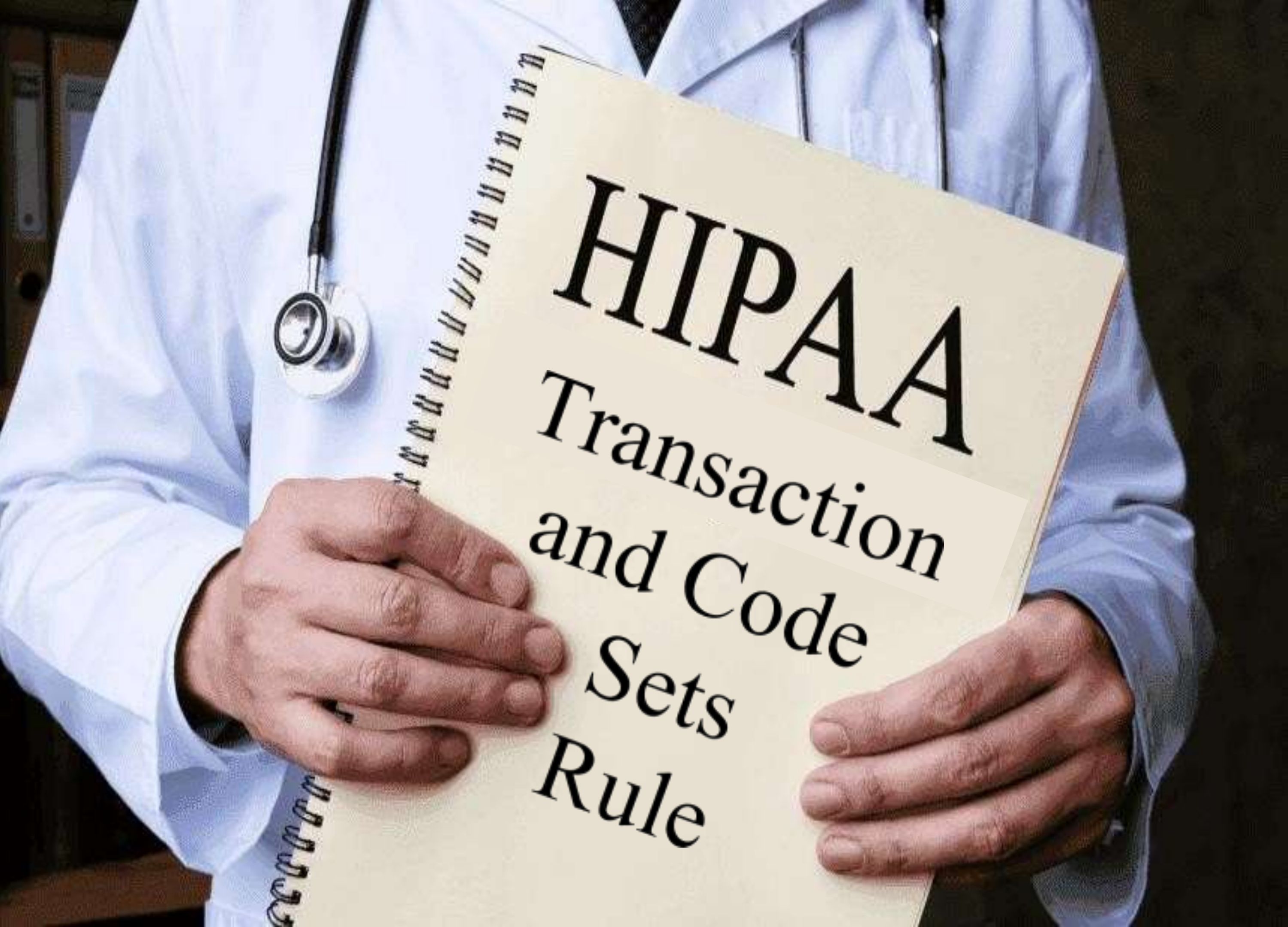
TECHNICAL SECURITY REQUIREMENTS

This rule aimed at protecting electronic protected health information (ePHI) and ensuring its confidentiality, integrity, and availability. These technical requirements provide guidelines for implementing safeguards within electronic information systems. Here are the key technical security requirements outlined in the HIPAA Security Rule:

- **ACCESS CONTROL - Implement technical measures to restrict access to ePHI based on the principle of least privilege. This involves assigning unique user identifiers, implementing authentication mechanisms (e.g., passwords), and enforcing access controls based on users' roles and responsibilities.**
- **AUDIT CONTROLS - Implement hardware, software, and procedural mechanisms to record and examine system activity. This includes generating audit logs that track access to ePHI and monitoring those logs for suspicious or unauthorized activities.**
- **INTEGRITY CONTROLS - Technical safeguards must be implemented to ensure the integrity of ePHI. This involves using methods like data hashing, digital signatures, and data validation to prevent unauthorized alterations or tampering.**
- **SECURITY INCIDENT PROCEDURES - Technical safeguards must include procedures for identifying and responding to security incidents involving ePHI. This involves promptly detecting and addressing unauthorized access or breaches.**

By setting comparable standards for electronic transactions and facilitating standardized code sets for diagnoses and other healthcare services, the HIPAA Transactions and Code Set Rule encourage a more efficient, accurate, and secure healthcare system.

Its purpose is to provide standards for electronic PHI exchanges. It covers various electronic transactions, including electronic data interchanges (EDI) and computer-to-computer exchanges with zero human involvement



PRIMARY TRANSACTIONS COVERED UNDER HIPAA TRANSACTION AND CODE RULE

Health Care Claims or Equivalent Encounter Information

- This transaction is used to submit healthcare claims, encounter information, or equivalent information for payment, which includes both professional and institutional claims.

Health Care Payment and Remittance Advice

- This transaction is used for electronic funds transfer (EFT) and remittance advice, allowing healthcare providers to receive payment information electronically.

Health Care Claim Status

- This transaction allows providers to inquire about the status of a healthcare claim to check whether it has been received, processed, or paid.

Enrollment and Disenrollment in a Health Plan

- This transaction is used by health plans to enroll and disenroll individuals, such as employees and dependents, in their health insurance plans.

Eligibility for a Health Plan

- This transaction provides information to healthcare providers about whether a patient is eligible for coverage under a specific health plan, including benefits and coverage details.

Health Care Electronic Funds Transfers (EFT) and Remittance Advice

- This is another transaction related to electronic funds transfers and remittance advice. It focuses on the electronic transfer of funds from a health plan to a provider.

Health Care Electronic Funds Transfers (EFT) and Remittance Advice Coordination of Benefits (COB)

- This transaction, like the previous one, deals with EFT and remittance advice but is specific to coordination of benefits, where more than one health plan is involved in a patient's coverage.

DIFFERENT CODES UNDER HIPAA TRANSACTION AND CODE SETS

ICD-9-CM

Stands for the International Classification of Diseases, 9th Revision, Clinical Modification.This is a standardized coding system used for medical diagnoses and inpatient hospital procedures in the United States. It was used extensively in the healthcare industry but has been largely replaced by ICD-10-CM. The codes in ICD-9-CM consist of alphanumeric characters and allow healthcare providers to document and communicate medical information in a standardized format. These codes were used for various purposes, including medical billing, epidemiology, and clinical research.

CPT-4

The Current Procedural Terminology, 4th Edition (CPT-4), is a standardized medical code set used in the United States to describe medical, surgical, and diagnostic services and procedures provided by healthcare professionals. CPT-4 codes are primarily used for: Billing and reimbursement and Documentation and communication.The use of CPT-4 codes is important in the healthcare industry for accurate billing, tracking medical procedures and services, and facilitating communication between healthcare providers, insurance companies, and government healthcare programs.

DIFFERENT CODES UNDER HIPAA TRANSACTION AND CODE SETS

CDT-2

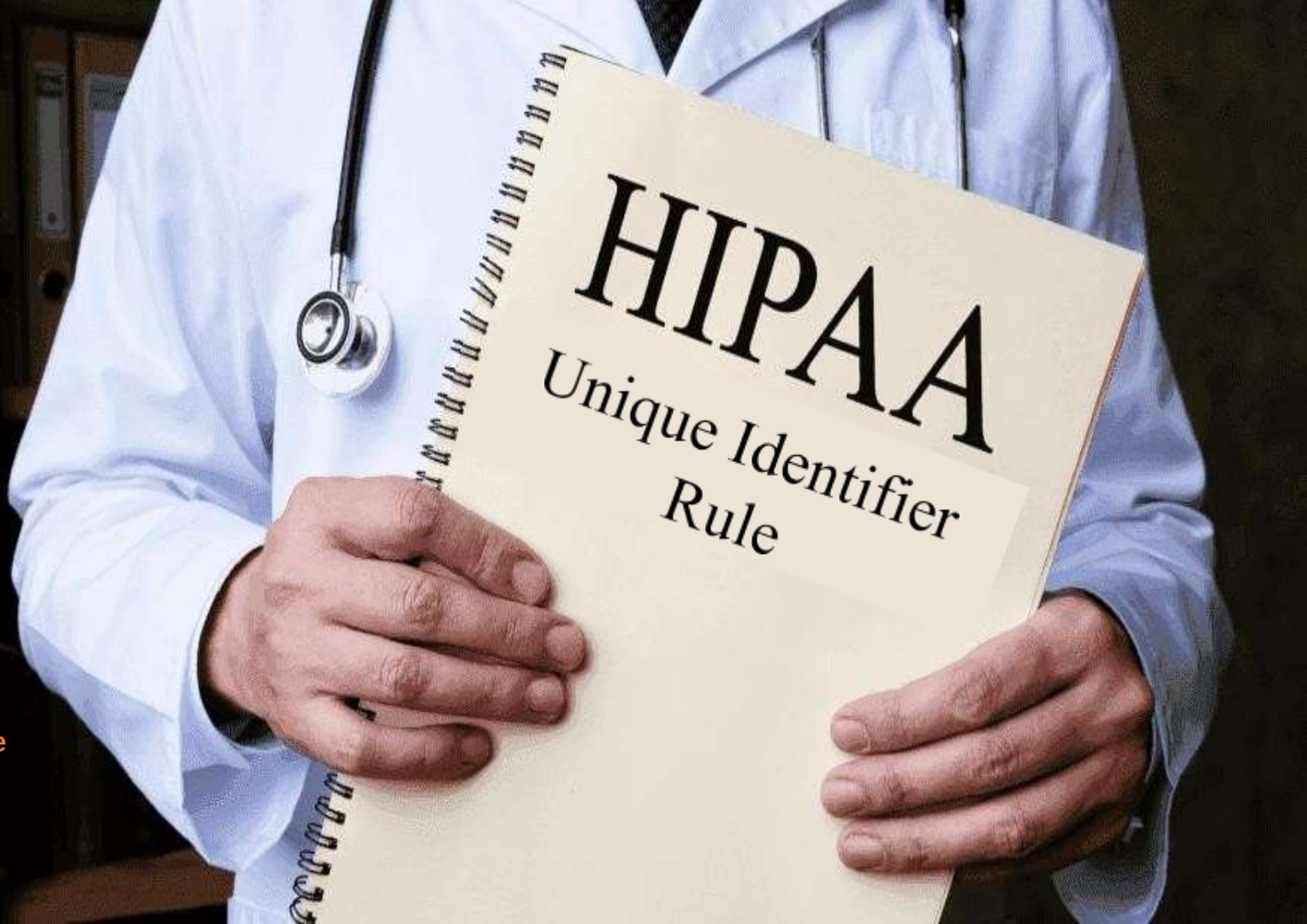
The Code on Dental Procedures and Nomenclature, also known as CDT-2, is a standardized code set published by the American Dental Association (ADA) for documenting and reporting dental procedures and services in the United States. CDT-2 is used primarily for dental billing, insurance claims, and the recording of dental procedures and services. CDT-2 codes are used by dentists, dental hygienists, dental assistants, and dental insurance companies to accurately describe and bill for dental treatments and services. These codes help ensure that dental procedures are documented consistently and that insurance claims are processed efficiently. Overall, CDT-2 is a valuable tool in the dental field, helping to standardize documentation and billing practices for dental services while ensuring that patients receive the appropriate insurance coverage and providers are properly compensated for their services.

NDC

The National Drug Code (NDC) is a unique identifier for medications, including prescription and over-the-counter drugs, as well as certain biological products, medical devices, and dietary supplements. The NDC system is used primarily in the United States to identify and label pharmaceutical products. NDC consists of three segments such as The labeler code, The product code and The package code. The FDA is responsible for assigning and managing NDCs, and the agency maintains a database of NDCs for various drug products. The NDC system is crucial for regulatory compliance, public health, and patient safety in the healthcare industry.

Covered entities get assigned identity codes. A set of unique digits that resemble specific entities in online systems. Unique identifiers allow covered healthcare providers and other entities to identify companies that also adhere to standard HIPAA transactions. The unique identifiers rule establishes different types of entity identifiers for varying transactions.

The use of these identifiers will promote standardization, efficiency and consistency.



FOUR MAJOR FORM OF UNIQUE IDENTIFIER

The Unique Identifiers Rule is essential for streamlining electronic transactions and protecting the privacy and security of patient information. It ensures that healthcare providers, health plans, and clearinghouses use a consistent and standardized method to identify and communicate with each other during electronic healthcare transactions.

NATIONAL PROVIDER IDENTIFIER (NPI)

The national provider identifier (NPI) is a unique 10-digit number assigned to individual healthcare providers and healthcare organizations. NPIs streamline the process of identifying providers across different health plans. They serve as universal identifiers, facilitating seamless, efficient electronic transactions between healthcare entities.

EMPLOYER IDENTIFICATION NUMBER (EIN)

The employer identification number (EIN) (assigned by the Internal Revenue Service) is a unique 9-digit number assigned to organizations. When conducting electronic healthcare transactions, employers provide their EIN as part of standard identifier information. EINs enable seamless coordination within the healthcare organization, ultimately benefiting patients by expediting the processing of claims and eligibility verification.

HEALTH PLAN IDENTIFIER (HPID)

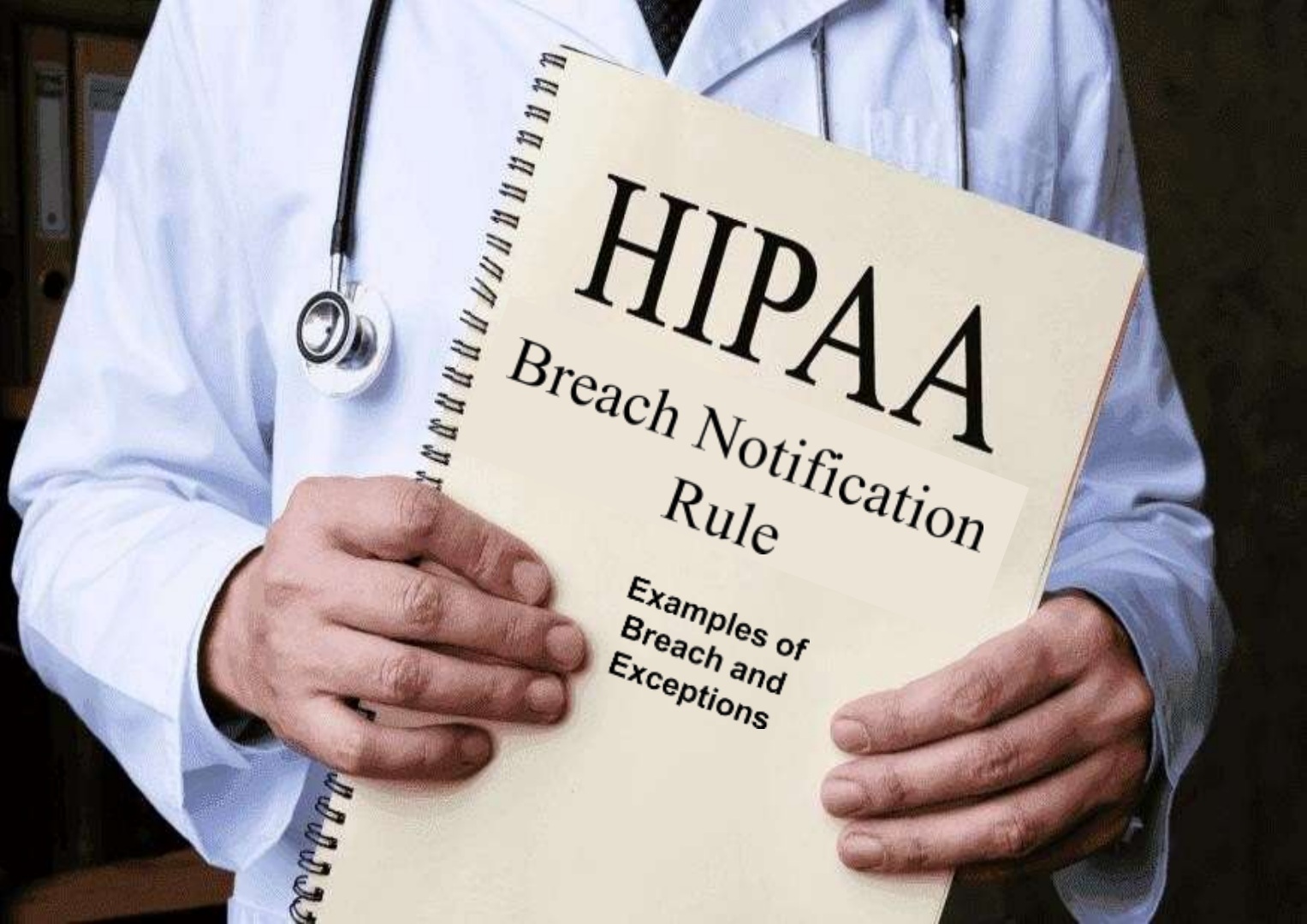
The purpose of a standard health plan identifier (HPID) was to uniquely identify a health plan. The government also adopted the other entity identifier (OEID). OEID functioned as voluntary identifiers for entities not labeled as health plans, healthcare providers, or individuals that need to be identified in HIPAA transactions.

UNIQUE PATIENT IDENTIFIER (UPI)

The unique patient identifier (UPI) is specifically for patients. UPIs serve as anonymous classifiers to help covered entities share health records with improved proficiency. Like other healthcare identifiers, the number is unique and does not contain PHI.

The Breach Notification Rule outlines the requirements for covered entities and their business associates to notify individuals, the U.S. Department of Health and Human Services (HHS), and in some cases, the media, in the event of a breach of protected health information (PHI).

The main goal of this rule is to ensure that individuals' health information is appropriately safeguarded and that they are informed in a timely manner if their PHI is compromised.



BREACH NOTIFICATION RULE

EXAMPLES OF HIPAA BREACH

- Patients have a right to their medical records within 30 days of a request; failure to provide them is a HIPAA violation.
- Organization uses or improperly discloses PHI.
- Losing a device or any records which exposes patient records to unauthorized individual.
- Improper disposal of PHI.
- Lack of encryption.
- Accessing PHI from unsecured location.

THE 3 HIPAA BREACH EXCEPTIONS

- If it was unintentional or done in good faith, and was within the scope of the authority.
- If it was done unintentionally between two people permitted to access the PHI.
- If the organization has a good faith belief that the person to whom the disclosure was made would not be able to retain the PHI.

HIPAA VIOLATION FINES

The violation of HIPAA (Health Insurance Portability and Accountability Act) can lead to multitude of severe punishments. In worst cases, violators could face imprisonment. The OCR is a primary federal department responsible for investigating and resolving breaches of HIPAA. They also conducts audits to review and determine if a covered entity is abiding by HIPAA safeguards.

What if it was determined that there wasn't compliance with HIPAA?

If OCR determine that there wasn't compliance with HIPAA, the OCR will attempt to resolve the situation in one of there three ways:

PENALTIES

TIER 1: Lack of Knowledge

TIER 2: Reasonable Cause

TIER 3: Willful Neglect, Corrected in 30 Days

TIER 4: Willful Neglect, Not Corrected in 30 days

Penalties

HIPAA Violation Penalty Tiers

THANK YOU

Stay Safe