# Health Insurance Portability and Accountability Act of 1996 (HIPAA)

**June, 2020**

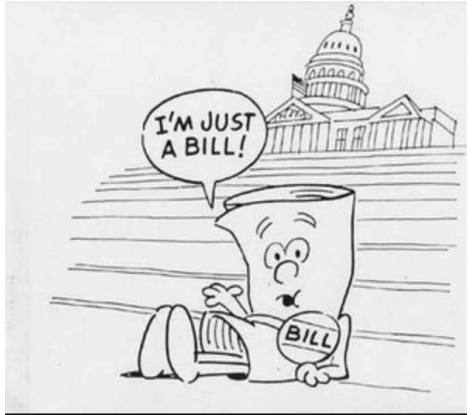

SerenaGroup

building the nation's leading wound care team.

# What is HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires the following:

- The ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs
- Reductions in health care fraud and abuse
- Industry-wide standards for health care information on electronic billing and other processes
- Protection and confidential handling of protected health information




SerenaGroup
Building the Nation's Leading Wound Care Team

# 5 Titles

- **Title I**: protects health insurance coverage for workers and their families when they change or lose their jobs
- **Title II:** known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers
- **Title III:** sets guidelines for pre-tax medical spending accounts
- **Title IV:** sets guidelines for group health plans
- **Title V:** governs company-owned life insurance policies

# Covered Entities


- **Healthcare providers:** Every healthcare provider, regardless of size of practice, who electronically transmits health information in connection with certain transactions. These transactions include claims, benefit eligibility inquiries, referral authorization requests, and other transactions for which HHS has established standards under the HIPAA Transactions Rule.
- **Health plans:** Entities that provide or pay the cost of medical care. Health plans include health, dental, vision, and prescription drug insurers; health maintenance organizations (HMOs); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government- and church-sponsored health plans, and multi-employer health plans.
- **Exception:** A group health plan with fewer than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity.
- **Healthcare clearinghouses**: Entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or healthcare provider as a business associate.
- **Business associates:** A person or organization (other than a member of a covered entity's workforce) using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity. These functions, activities, or services include claims processing, data analysis, utilization review, and billing.

# Privacy VS Security

**Privacy** is the right of an individual to keep his/her individual health information from being disclosed.

**Security** is how we prevent PHI from accidental or intentional disclosure, alteration, destruction or loss.

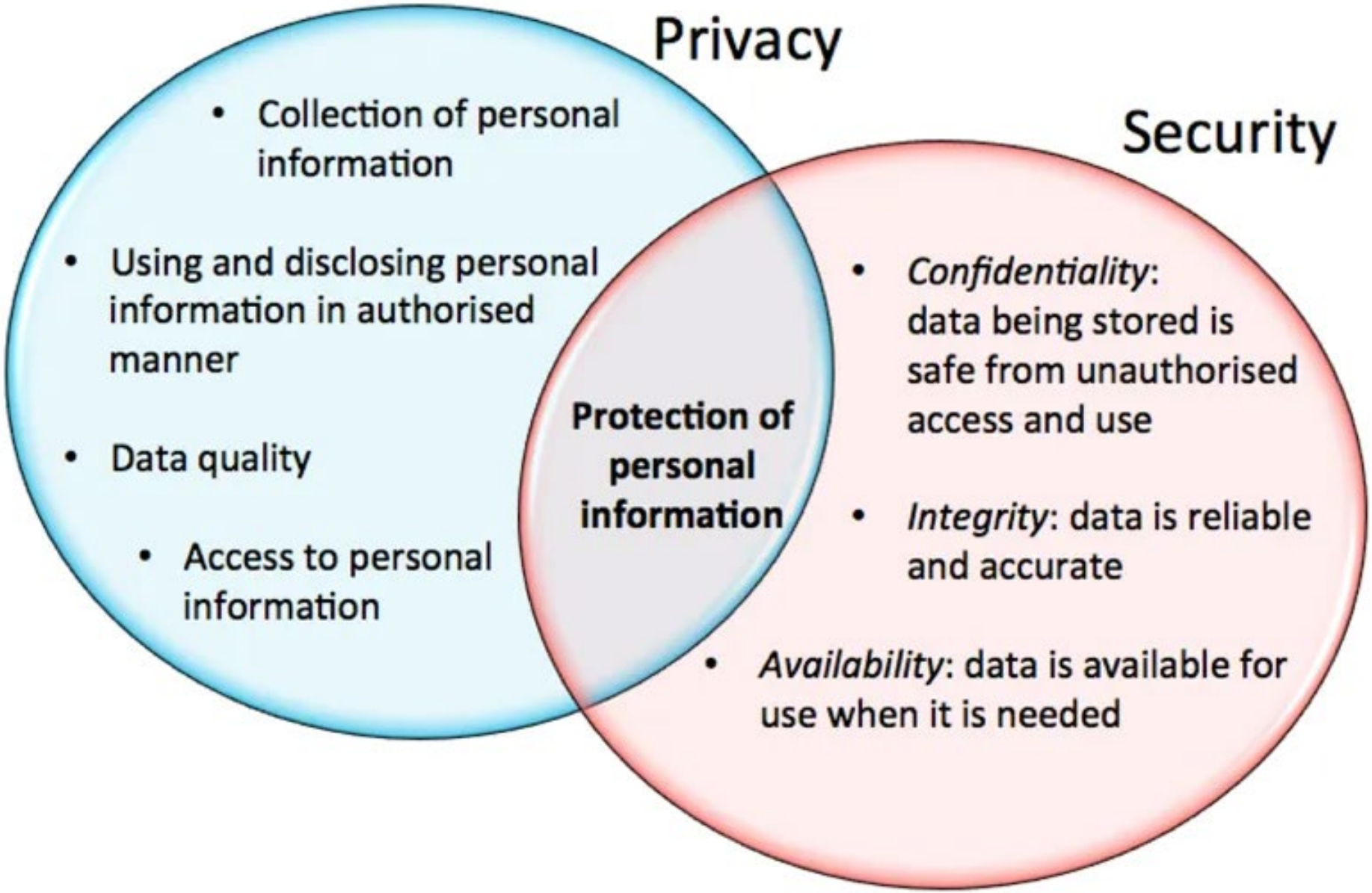
SerenaGroup
Building the Nation's Leading Wound Care Team

# HIPAA Privacy Rule

- The Privacy Rule standards address the use and disclosure of individuals' health information (known as "protected health information") by entities subject to the Privacy Rule. These individuals and organizations are called "**covered entities**." The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used. A major goal of the Privacy Rule is to ensure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.

# HIPAA Security Rule

- While the HIPAA Privacy Rule safeguards protected health information (PHI), the Security Rule protects a subset of information covered by the Privacy Rule. This subset is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is called “electronic protected health information” (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.
- To comply with the HIPAA Security Rule, all covered entities must do the following:
  - Ensure the confidentiality, integrity, and availability of all electronic protected health information
  - Detect and safeguard against anticipated threats to the security of the information
  - Protect against anticipated impermissible uses or disclosures
  - Certify compliance by their workforce
  - Covered entities should rely on professional ethics and best judgment when considering requests for these permissive uses and disclosures. The HHS Office for Civil Rights enforces HIPAA rules, and all complaints should be reported to that office. HIPAA violations may result in civil monetary or criminal penalties.




SerenaGroup
Building the Nation's Leading Wound Care Team

# Permitted Uses and Disclosures

- **A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:**
- **Disclosure to the individual (if the information is required for access or accounting of disclosures, the entity MUST disclose to the individual)**
- **Treatment, payment, and healthcare operations**
- **Opportunity to agree or object to the disclosure of PHI (Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object)**
- **Incident to an otherwise permitted use and disclosure**

- **Public interest and benefit activities—The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes:**
  - **When required by law**
  - **Public health activities**
  - **Victims of abuse or neglect or domestic violence**
  - **Health oversight activities**
  - **Judicial and administrative proceedings**
  - **Law enforcement**
  - **Functions (such as identification) concerning deceased persons**
  - **Cadaveric organ, eye, or tissue donation**
  - **Research, under certain conditions**
  - **To prevent or lessen a serious threat to health or safety**
  - **Essential government functions**
  - **Workers compensation**

# Need to know

**HIPAA's "Minimum Necessary" rules :**

- Must provide only PHI in the minimum necessary amount

to accomplish the purpose for which use or disclosure is sought

- Minimum necessary does not apply when patient provides a valid, signed authorization for release of PHI
- De-identified Information: De-identified information is PHI with all HIPAA identifiers removed.

***Exceptions*:**

- Disclosure to a health care provider for treatment
- permissible uses or disclosures made by the patient.
- Uses or disclosures made based on patient's signed authorization.
- Uses or disclosures required for HIPAA compliance
- Use for legal proceedings, law enforcement, etc.

SerenaGroup
Building the Nation's Leading Wound Care Team

# HIPAA COMPLIANCE FOR A DOCTOR'S OR DENTIST'S OFFICE

## CULTURE OF PATIENT PRIVACY

Exercise privacy in your office **EVERYWHERE**

Display Notice of Privacy Practices **PROMINENTLY** in office & on website

Exercise caution in use and disclosure of **PHI** (PROTECTED HEALTH INFORMATION)

## SECURITY and PRIVACY REQUIREMENTS

Conduct mandatory annual **RISK ASSESSMENT**

Maintain and follow security & privacy **POLICIES & PROCEDURES**

Conduct **HIPAA TRAINING** for your staff & physicians every year

# Requirements of Notifications

Purpose: to provide consumer with adequate notice of uses or disclosures of PHI

- Must be written in plain language
- Must be provided at the time of first service or assessment for eligibility
- Has to provide Privacy Officer contact information


SerenaGroup
Building the Nation's Leading Wound Care Team

# Consumer Protection

## Access

- Consumers can access, inspect and copy PHI
- Request for access MUST be in writing
- Facility Must - Respond to request within 60 days;
- May recover cost-based fee for copy, explanation, or summary of records
- If access is denied, reason for that denial will determine if the consumer can appeal
- Consumer must appeal to facility Privacy Official

# Consumer Protection

## Restriction

- Consumers may request that the facility restrict how it uses/discloses their PHI
- Facility is not required to accept the request
- If restriction request is accepted the facility may not deviate or depart from that restriction

# Consumer Protection

## Amendment

- Consumers may request to amend PHI in medical records
- That request may be referred to the facility Privacy Official

# Play it Safe

1. When in doubt, don’t give information out
2. Log off before you walk off from your computer
3. Double check fax numbers before sending
4. Do not send e-mails or use the internet unless the connection is secure and approved
5. Identify the caller before releasing confidential information over the phone
6. Never share your password with anyone
7. Maintain the security of all patient information in all forms (electronic, print, verbal)
8. Discuss patient information in private locations
9. Access information on a need to know basis
10. Properly dispose of printed PHI in a dedicated locked contained for shredding

SerenaGroup
Building the Nation's Leading Wound Care Team


- OCR Issues Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information about Individuals in Their Facilities - May 5, 2020
- OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency - April 9, 2020
- OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency - April 2, 2020
- OCR Issues Bulletin on Civil Rights Laws and HIPAA Flexibilities That Apply During the COVID-19 Emergency - March 28,2020
- OCR Issues Guidance to Help Ensure First Responders and Others Receive Protected Health Information about Individuals Exposed to COVID-19 - March 24, 2020
- OCR Issues Guidance on Telehealth Remote Communications Following Its Notification of Enforcement Discretion - March 20, 2020
- OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency - March 17, 2020

SerenaGroup
Building the Nation's Leading Wound Care Team

# Enforcement Discretion to Allow Uses and Disclosures

The Office for Civil Rights (OCR) at the U.S Department of Health and Human Services (HHS) announced, that it will exercise its enforcement discretion and will *not impose penalties* for violations of certain provisions of the HIPAA Privacy Rule against health care providers or their business associates for the good faith uses and disclosures of protected health information (PHI) by business associates for public health and health oversight activities during the COVID-19 nationwide public health emergency.

"The CDC, CMS, and state and local health departments need quick access to COVID-19 related health data to fight this pandemic," said Roger Severino, OCR Director. "Granting HIPAA business associates greater freedom to cooperate and exchange information with public health and oversight agencies can help flatten the curve and potentially save lives," Severino added.

# Guidance on Telehealth

The OCR is exercising its enforcement discretion to *not impose penalties* for HIPAA violations against healthcare providers in connection with their good faith provision of telehealth using communication technologies during the COVID-19 nationwide public health emergency.

"We are empowering medical providers to serve patients wherever they are during this national public health emergency," said Roger Severino, OCR Director. "We are especially concerned about reaching those most at risk, including older persons and persons with disabilities," Severino added.


Take the
HIPAA Quiz!
Quiz

Name_____ Date_____

1. The Health Insurance Privacy and Portability Act of 1996 includes 5 titles and extends beyond just the protection of sensitive health information
    a. True
    b. False
2. HIPAA Privacy is defined as;
    a. The right of an individual to keep their individual health information from being disclosed
    b. The way in which PHI protected against intentional or accidental disclosure
    c. A patient's right to view their medical record
    d. A patient's right to make amendments to their medical record
3. HIPAA Security is defined as;
    a. The prevention on PHI from accidental or intentional disclosure, alteration, destruction or loss
    b. An individual's right to keep their individual health information from being disclosed
    c. A patient's right to view their medical record
    d. A patient's right to make amendments to their medical record

Name_____ Date_____

1. One exemption of the “minimum necessary” rule is;
    a. Disclosure to a healthcare professional for treatment purposes
    b. If you think the person receiving the information is trustworthy
    c. If you feel that the person would like to know even though they do not need to know
    d. If the person promises not to share the information with anyone else
2. A Physician’s office can help ensure HIPAA compliance by
    a. Building a culture of privacy and following all security and privacy requirements
    b. By making menacing threats to anyone who might break the rules
    c. By never sharing any PHI at al
    d. By stating that they have an open communication policy and patients enter at their own risk
3. Physician offices must post a privacy statement in a common area for all patients to see
    a. True
    b. False
4. Patients may provide a written request to prevent some individuals from accessing their personal information
    a. True
    b. False

Name_____ Date_____

1. One way you can ensure PHI is secure is to
    a. Never share your computer passwords and to log out before leaving your work station
    b. Only sharing your passwords with your best friends at work
    c. By asking patients to keep an eye on your work station while you walk away
    d. Avoid using computers at all costs
2. During the COVID-19 pandemic, the enforcement of certain HIPAA regulations have been relaxed
    a. True
    b. False
3. The relaxation of HIPAA regulations (for our purposes) only apply to the good faith use of
    a. Both B +C
    b. Telehealth platforms to ensure access to care
    c. Timely communication with Health Departments and other government agencies
    d. Allowing staff to snoop around to see who has been infected