

Health Information Privacy



September 27, 2018

**Paddy DiPadova
JSI Senior Consultant**

Your presenter



Paddy DiPadova, MPH
Senior Consultant
JSI

Pretest

- 1) HIPAA only applies to covered entities which include:
 - a) health plans
 - b) health care providers
 - c) health care clearinghouses
 - d) all of the above

- 2) Which one of the following is required to be included in a privacy notice by a covered entity:
 - a) A list of providers the protected health information (PHI) could be shared with
 - b) A copy of the entire HIPAA legal document
 - c) How the Covered entity may use and disclose PHI





1. Build awareness of privacy and civil rights laws including HIPAA
2. Explain patient privacy requirements and guiding principles
3. Describe the responsibilities of a Covered Entity

TAKEAWAYS

Use Common Sense

Handle health information for others the way you would want your health information handled

Policies and Procedures

Documentation

Privacy and Civil Rights Laws

Federal Laws

- HIPAA
- Confidentiality of Alcohol and Drug Abuse Patient Records
 - 42 CFR Part 2 (Referred to as “Part 2”)
- Title II of the Americans with Disabilities Act (ADA)
- Family Educational Rights and Privacy Act (FERPA)



State Laws

- Confidentiality – such as Doctor/Patient and Therapist/Patient Privileges; Communicable Disease Reporting
- Minor Consent Laws

Poll: How comfortable do you feel about HIPAA as relates to your work?

- a) Extremely comfortable
- b) Somewhat comfortable
- c) I don't know anything about it

Health Insurance Portability And Accountability Act of 1996 (HIPAA)

1. Privacy
2. Security
3. Identifiers
4. Transactions and Code Sets
5. Enforcement



Sources: 45 CFR Parts 160, 162 & 164 and Section 13401 of Subtitle D (Privacy) of the HITECH Act (42 USC 17931)

Health

Insurance

Portability

Accountability

Act



HIPAA Privacy Rule

National standards to protect medical records and other personal health information

Sets standards for when health information can be shared: “Permitted Uses and Disclosures”

- Covered Entity
- Business Associate
- Protected Health Information (PHI)

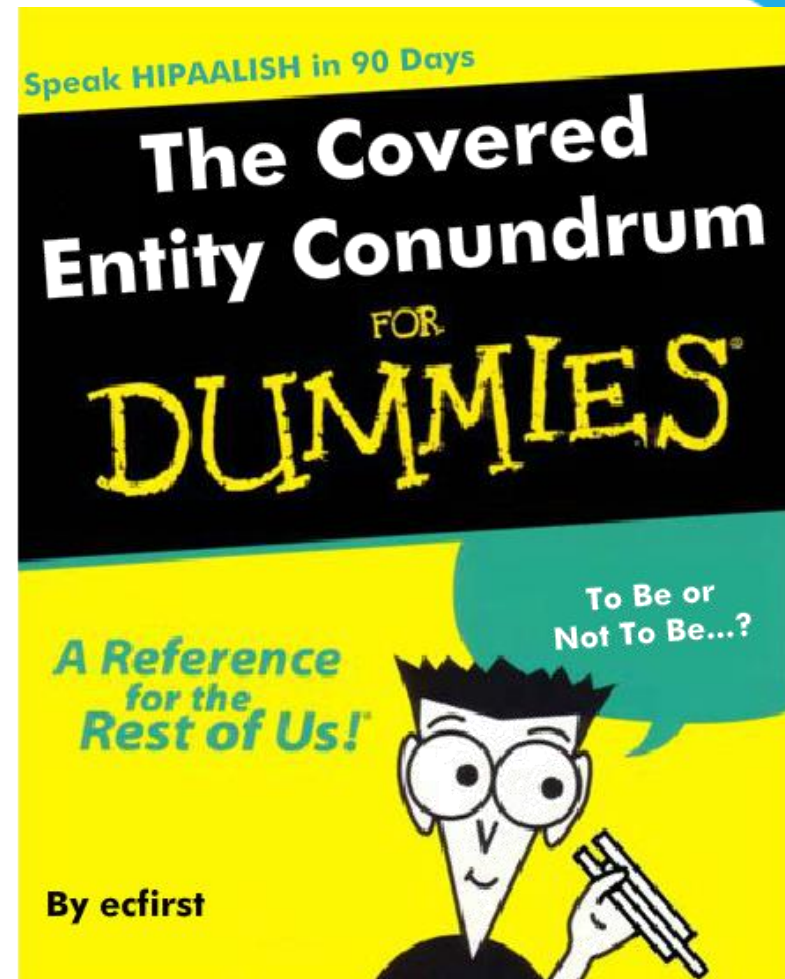


Covered Entities

Health Plans

Health Care Providers

Health Care Clearinghouses



Covered Entities: Health Plans

An individual or group plan that provides, or pays for the cost of, medical care.

- Health Insurers
- Managed Care Organizations
- Government Organizations (e.g., Medicaid, Medicare, and the Veterans Health Administration)

Health
Plan

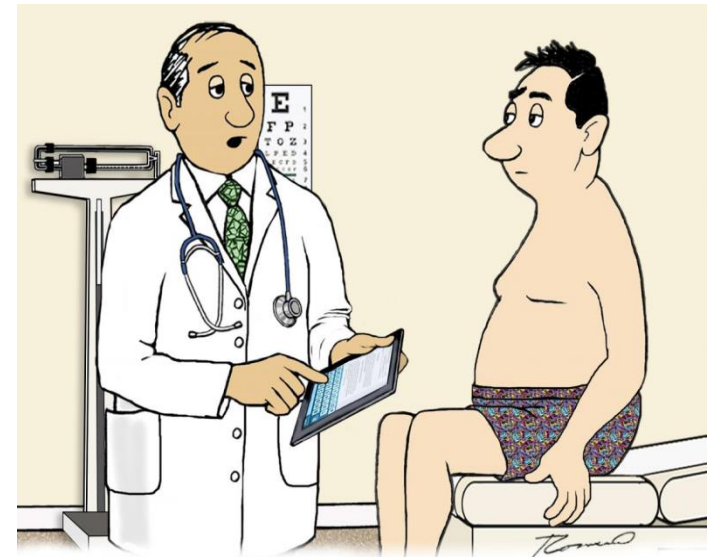


Covered Entities: Health Care Providers

Person or organization that furnishes, bills, or is paid for health care in the normal course of business,

and

Transmits health information in electronic form.



"According to your HIPAA release form
I can't share anything with you."

Covered Entities: Health Care Clearinghouse

Public or private entity that processes data received from another entity into a different format.

Example: Billing service that processes data into a standardized billing format



Covered Entity Guidance Tool

CMS Tool to Assist in Identifying Covered Entity Status

<https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf>



Covered Entity Guidance

Find out whether an organization or individual is a covered entity under the Administrative Simplification provisions of HIPAA



Poll: Have you ever used the CE Guidance tool?

Yes

No

Business Associate



A person or entity that performs certain functions or activities that involve the use or disclosure of Protected Health Information on behalf of, or provides services to, a Covered Entity.

Examples:

- An independent data entry person that enters client data on behalf of a Healthy Start worker.
- An enrollment specialist that enrolls a participant in a health insurance plan

Covered Entity's Responsibility

Covered Entities must obtain satisfactory assurances that the BA will

- use the information only for the purposes for which it was engaged by the covered entity
- safeguard the information from misuse
- help the covered entity comply with some of the covered entity's duties under the Privacy Rule

Business Associate Agreement (BAA)

Satisfactory assurances must be in writing

- Describe the permitted and required uses of PHI by BA
- Require BA to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided in BAA

Sample BAA at

<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>



Protected Health Information (PHI)

- 1) Created or received by a Covered Entity;
- 2) Relates to
 - the past, present, or future physical or mental health or condition,
 - provision or payment of health care of an individual; and
- 3) Identifies the individual; or there is a reasonable basis to believe the information can be used to identify the individual

Source: 45 CFR 160.103



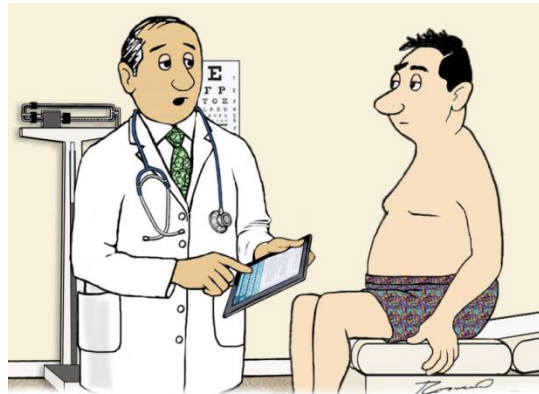
De-Identifying PHI

1. Names
2. All geographic subdivisions smaller than a state except for the initial three digits of a zip code if, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people
3. All elements of dates (except year)*
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locator (URL)
15. Internet protocol (IP) address number
16. Biometric identifiers, including finger or voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code.



Permitted Uses and Disclosures

1. To the individual
2. Treatment, payment or operations (TPO)
3. With valid authorization
4. For a facility directory or sharing information with a relative, close friend or other person identified by the individual.
5. Where the Uses and Disclosures do not require consent, authorization or an opportunity to agree or object



"According to your HIPAA release form
I can't share anything with you."

When Consent is Not Required

To avert a serious threat to health or safety

As required by law

For public health activities

To coroners, medical examiners and funeral directors

For cadaveric organ, eye or tissue donation

For specialized government functions, including military and veterans activities

For workers' compensation



HIPAA Covered Entity Requirements



If you are a Covered Entity, You Must:

Appoint a privacy officer

Develop minimum necessary policies and procedures to obtain consent or authorization for releases of personal health information

Amend Business Associate contracts

Develop an accounting of disclosures capability

Develop a procedure to request alternative means of communication

Develop a procedure to request restricted use

Develop a complaint procedure

Develop an amendment request procedure

Develop an access, inspection, and copying procedure

Develop an anti-retaliation policy

Train the workforce

Develop and disseminate a privacy notice



Privacy Notice



Privacy Notice

Content

- How the CE may use and disclose PHI
- Individual rights with respect to the PHI, complaints
- CEs legal duties with respect PHI
- Contact info for further information about CEs privacy policies
- Effective Date

Required to revise and distribute if any material changes are made to privacy practices

45 CFR 164.520(b) – for specific requirements



Model Privacy Notices


Booklet, layered notice, full page, text only

Provider Instructions

English, Spanish

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html>


HHS.gov U.S. Department of Health & Human Services
Health Information Privacy

I'm looking for... 

[HHS A-Z Index](#)

 **HIPAA for Individuals**


 **Filing a Complaint**

 **HIPAA for Professionals**

 **Newsroom**

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Privacy](#) > [Guidance](#) > Model Notices of Privacy Practices


HIPAA for Professionals

Privacy 

[Summary of the Privacy Rule](#)

[Guidance](#)

[Combined Text of All Rules](#)

Text Resize 

Print 

Share   

Model Notices of Privacy Practices

The HIPAA Privacy Rule requires health plans and covered health care providers to develop and distribute a notice that provides a clear, user friendly explanation of individuals rights with respect to their personal health information and the privacy practices of health plans and health care providers. This page provides options for meeting the requirement to create notices of privacy practices (NPP).

HHS developed the model NPPs you see on this site to help improve patient experience and



Poll: Privacy Notices

Do you have a sample privacy notice that you'd be willing to share with other grantees?

Yes

No

Privacy Notice Distribution

CEs with Direct Treatment Relationship

- 1st encounter – patient visits
- Electronically – patient portal or other electronic service
- Prompt mail – telephone service
- Post at all service delivery sites
- Posted on web site
- Available on request to anyone who asks for it
- In an emergency – made available as soon as practicable
- Good faith effort to get acknowledgement of notice receipt

Enforcement



Non-Compliance Penalties

HIPAA is serious business

Can be financial and criminal penalties for non-compliance

Penalties can be applied even if there is not breach of PHI, but there is non-compliance

- i.e. no BAA in place

Ignorance of HIPAA Rules is no excuse for a rule violation



Breach Responsibilities

Conduct a breach risk assessment

Notification of impacted individuals

Exceptions:

1. Unintentional use by workforce member acting under authority of CE or BA, made in good faith and within the scope of authority
2. Inadvertent disclosure by an authorized person to another authorized person

In both cases, PHI cannot be further used or disclosed

3. Good faith belief that unauthorized person receiving PHI would not be able to retain it



Remember



PHI can be disclosed for:

- Treatment, Payment and Operations
- To prevent an imminent threat
- For identification, location and notification

In all circumstances:

- Best to get consent where possible.
- Limit the PHI provided to the minimum necessary to get the job done
- Have policies and procedures in place

Questions?



Post-test

- 1) HIPAA only applies to covered entities which include:
 - a) health plans
 - b) health care providers
 - c) health care clearinghouses
 - d) all of the above

- 2) Which one of the following is required to be included in a privacy notice by a covered entity:
 - a) A list of providers the PHI could be shared with
 - b) A copy of the entire HIPAA legal document
 - c) How the Covered entity may use and disclose PHI



Next Steps and Reminders

Upcoming Webinars:

- October 9 : 3-4pm ET - *The Fourth Trimester: A new paradigm for preventing maternal mortality*

Discussion Groups:

- *Certified Lactation Counselors: October 11 – 1-2:30pm*
- *Fatherhood and Male Involvement Coordinators: October 16 and November 20 – 1-2:30pm*
- *Evaluator Listserv (coming soon)*

EPIC Center website: <http://www.healthystartepic.org>

Includes all recorded webinars, transcripts, and slide presentations

