
KANSAS HOSPITAL
KHA
ASSOCIATION

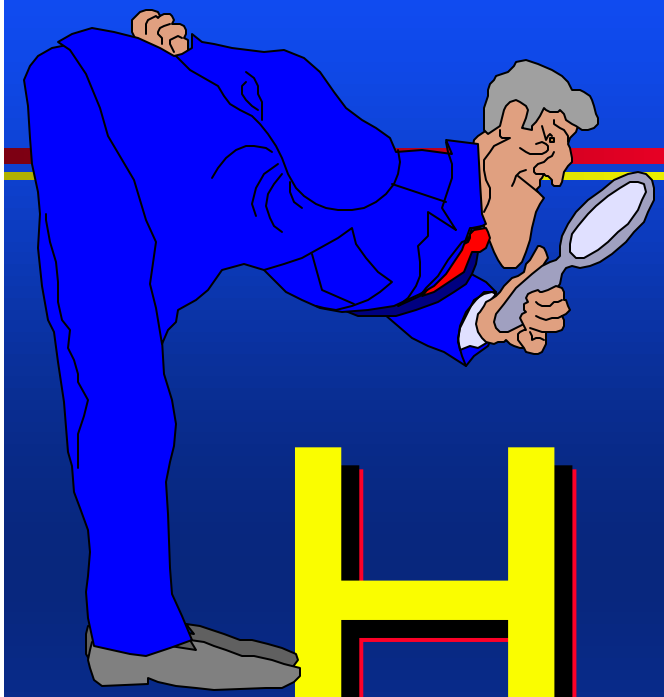
# HIPAA PRIVACY STANDARDS

# A Practical Guide to HIPAA PRIVACY REGULATION COMPLIANCE

by

GOODELL, STRATTON,

EDMONDS & PALMER, L.L.P.



# HIPAA

# The Health Insurance Portability and Accountability Act of 1996

- Portability

  1. Portability of health insurance for employees changing jobs.

  2. Prohibiting discrimination based on health.

  3. Loosening pre-existing condition restrictions imposed by health plans.

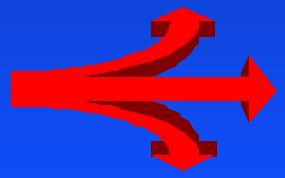
Table A-1

# The Health Insurance Portability and Accountability Act of 1996

- ACCOUNTABILITY / ADMINISTRATIVE SIMPLIFICATION

  45 C.F.R., Subtitle A, Subchapter C:

  - Standardized data formats and use identifiers necessary to improve the electronic data interchange of health information among providers, health plans and clearinghouses.



# The Health Insurance Portability and Accountability Act of 1996

- ACCOUNTABILITY / ADMINISTRATIVE SIMPLIFICATION
  - **Protect the privacy of the patient's health information**
  - Provide adequate security for systems used to maintain or store such information.
  - Allow for electronic signatures to be used in the health care industry.

Table A-1

# HIPAA: SCOPE - Three major areas of privacy regulation

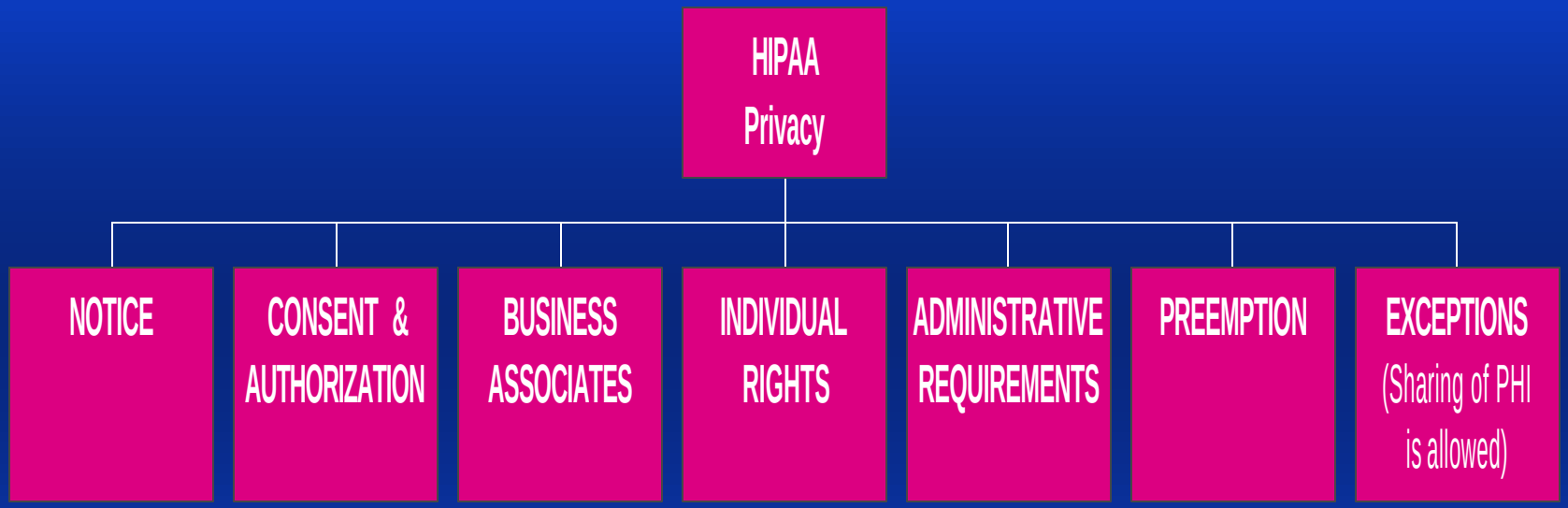
1. Use and disclosure of protected health information.
2. The individual (patient) rights with regard to protected health information.
3. Administrative requirements and safeguards that must be established to protect privacy. Table A - 6

# Privacy Laws

# Examples of Privacy / Confidentiality "Laws"

- KDHE Patient Rights K.A.R. 28-34-3b
- Medicare Conditions of Participation, sec. 482.13
- JCAHO, IM.2-2.3
- Privacy Act of 1974
- Institutional Review Boards
- Confidentiality of Alcohol & Drug Abuse Records, 42 CFR Part 2
- State Laws
- Federal Laws
- Standards of Practice
- Case Law

# HIPAA Privacy Overview



# HIPAA Privacy Overview

- 160.103 contains key definitions for use of HIPAA.
- 164.501 contains definitions specifically related to the privacy standards.
- 164.502 sets forth the “general rules” for uses & disclosures of PHI. (to be read with 506 & 508 & 520)
- 164.512 lists exceptions as to when PHI can be released. (to be read with 510)
- 164.514 contains requirements for use & disclosure.
- 164.522 addresses specific individual rights (with 524 & 526).
- 164.530 outlines the administrative requirements.

# Definitions for HIPAA

45 C.F.R. 164.501

**Use:** Means with respect to individually identifiable health information (PHI), the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

***Use within a facility / provider***

# Definitions for HIPAA

45 C.F.R. 164.501

**Disclosure:** Means the release, transfer, provision of access to, or divulging in any other matter of information outside the entity holding the information.

***Release outside the facility / provider***

# Definitions for HIPAA

45 C.F.R. 164.501

**Protected Health Information**: **(PHI)**

Means individually identifiable health information * ..... transmitted or maintained ....in any ... form or medium.

* relates to past, present, or future physical or mental health or condition of an individual & identifies the individual.

# Definitions for HIPAA

45 C.F.R. 164.501

**Designated Record Set: A group of records maintained by or for a covered entity that is the medical records, billing records, ... used, in whole or in part, by or for the covered entity to make decisions about individuals. (Record means any item, collections, or grouping of information that includes PHI.)**

# Definitions for HIPAA

45 C.F.R. 164.501

**Treatment:** Means the provisions, coordination, or management of **health care** and related services by one or more health care providers, including the coordination or management of health care by a **health care provider** with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

# Definitions for HIPAA

45 C.F.R. 160.103

**Health care:** Means care, services, or supplies related to the health of an individual. Health care includes but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure of the body; **and**

# Definition of "Health Care" *(con't)*

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

---

**Health Information:** Means any information, oral or recorded in any form or medium, that is created or received by a health care provider(s) (& others) **AND**

# Definition of Health Information

**Health Information:** Means any information, oral or recorded in any form or medium, that is created or received by a health care providers (& others) **AND**

**Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.**

# Definition of
# Health Care Operations

45 C.F.R. 164.501

Appendix B, page 11

QA ..... Case Management & Care Coordination ..... Treatment alternatives ..... Reviewing competence, qualifications or performance of health care providers ..... Training Programs in health care ..... Accreditation & Licensing & Credentialing .....

Conducting or arranging for medical review, legal services, & auditing ..... Business management & general administrative activities of the CE.

# Minimum Necessary

45 C.F.R. 164.502(b) & 514(d)

- A CE can only use or disclose PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure, or request.
- This does NOT apply to disclosures to or request by a health care provider for treatment, to an individual, or disclosures required by law.

# Minimum Necessary

- Must have policies & procedures that identify the persons or class of persons in the workforce who need access to PHI to carry out their duties **PLUS** the category or categories of PHI to which such persons or classes need access **AND** the conditions that would apply to such access.

# Minimum Necessary

- The CE must also have a policy & procedure that addresses routine, recurring disclosures that permit only the disclosure of the minimum PHI reasonably necessary to achieve the purpose of the disclosure .....

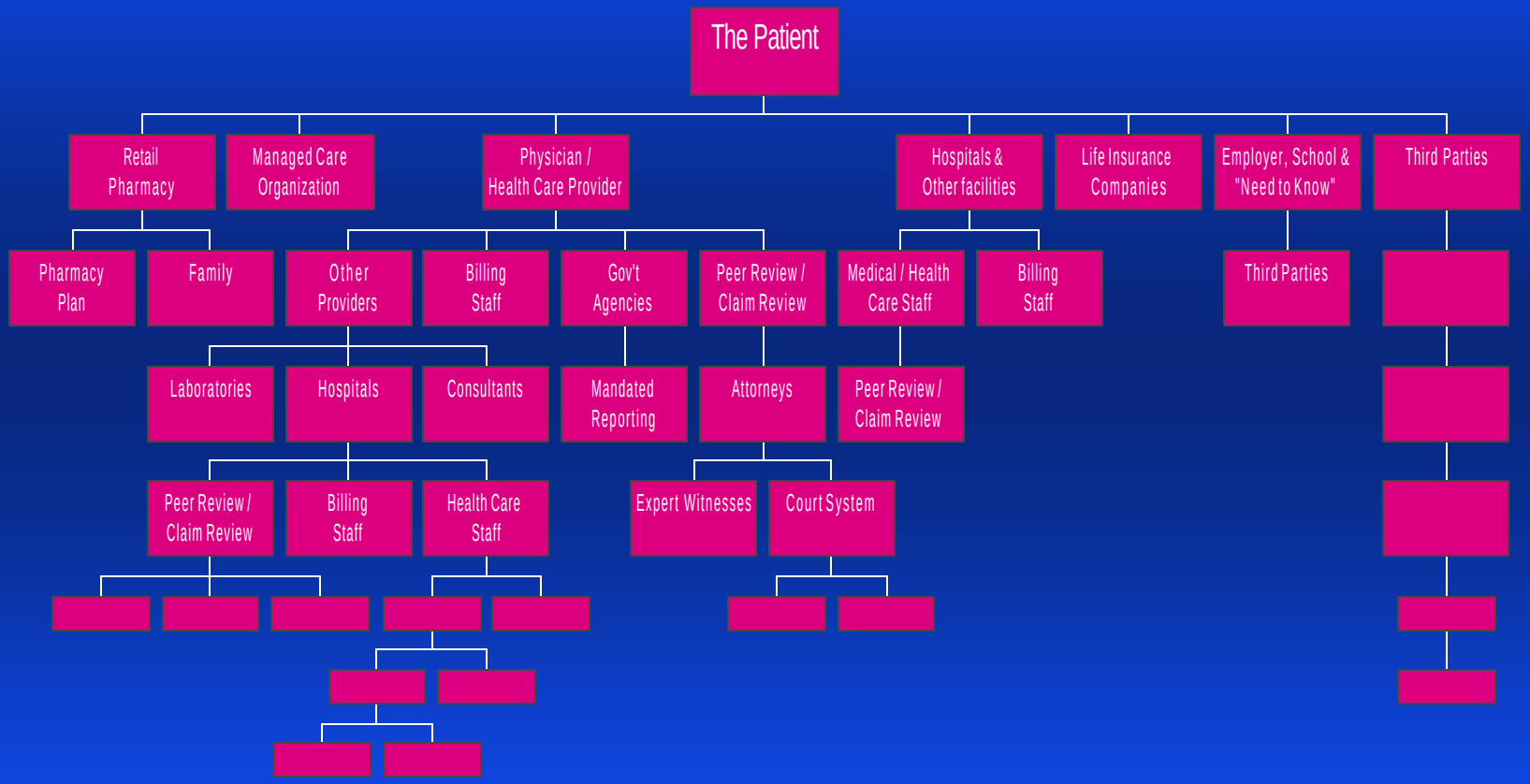
Designate type of PHI ... type of persons who would receive the PHI .... and the condition that would apply to the access.

# Minimum Necessary

- For all other disclosures (non-routine) the CE must develop "criteria" designed to limit the PHI to that reasonably necessary.....**AND review such requests on an individual basis.**

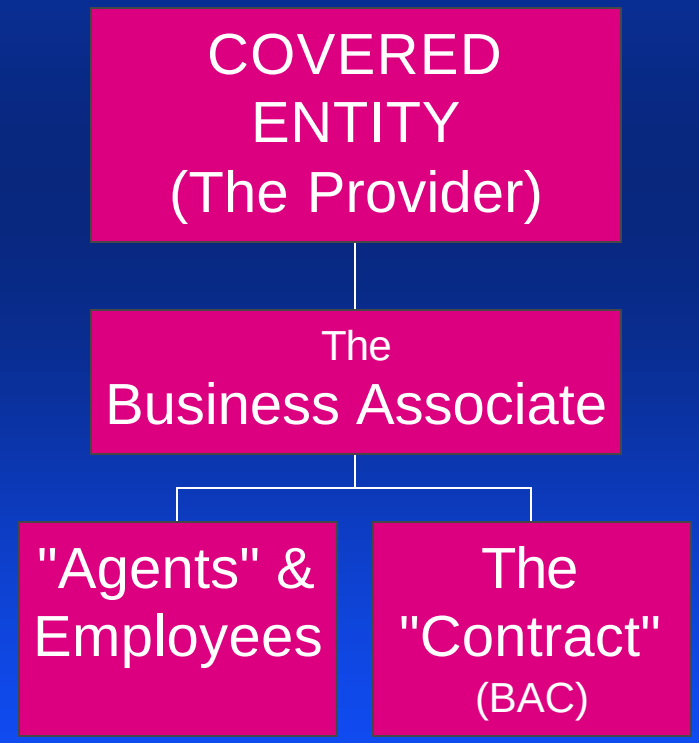
# "Types" of Medical Records

# PHI and where it goes ....



# BUSINESS ASSOCIATES & PHI

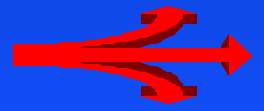
45 C.F.R. 164.502(e)



# "Use and Disclosure" of PHI
## (Permitted - Table 16)

45 C.F.R. 164.502(a)

- To an Individual
- By a **consent** to carry out treatment, payment & health care operations.
- Without consent in certain situations.
- By an **authorization.**
- Facility Directory or to family member / friend involved in the individual's health care.



# "Use and Disclosure" of PHI
## (Permitted - Table 16)

- Under any **exception** *("as required by law, abuse, health oversight, law enforcement, .....)*, marketing, fundraising or underwriting.
- "Business Associates" *[not under 164.502(a) put permitted under 502(e)]*

# "Use and Disclosure" of PHI

## (*Required* - Table 16)

45 C.F.R. 164.502(a)(2)

- To an individual when requested under 164.524 or 164.528
- When required by HHS to investigate or determine the CE's compliance with this provision of HIPAA.

# The "Notice"

45 C.F.R. 164.520

**The individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the provider and how to exercise the individual's rights relating to the PHI and the use and disclosure of the PHI.** **Table A-9**

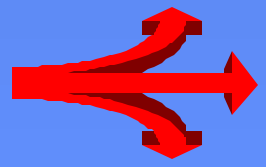
**"What are you going to do with this information & what can I do about it?"**

# The "Notice": Who, what, where, when, and how.

1. Provided to the individual no later than the first service delivery.
2. Provided upon request.
3. Posted so it can be seen.
4. Posted prominently on & made available electronically through the provider's web site (if the site provides information about the provider's customer services or benefits)

# The "Notice" .....

- Must be in plain easy to understand language.
- A description **AND** AN **EXAMPLE** of the types of uses & disclosures made for treatment, payment & health care operations. These "examples" will be specific to each health care provider.



# The "Notice" .....

- ❼ A description of EACH of the other purposes for which the provider is permitted or required to use or disclose PHI without the individual's written consent or authorization.
- ❽ Required "statements" and required "magic" language used as a header. Table A-10

# Release of PHI

- A **"Consent"** is only effective for a limited number of *uses and disclosures.*
- An **"Authorization"** can be used for any number of proposed disclosures.

# Consents

45 C.F.R. 164.506

Drafted in General Terms.

Provided at same time with the "Notice."

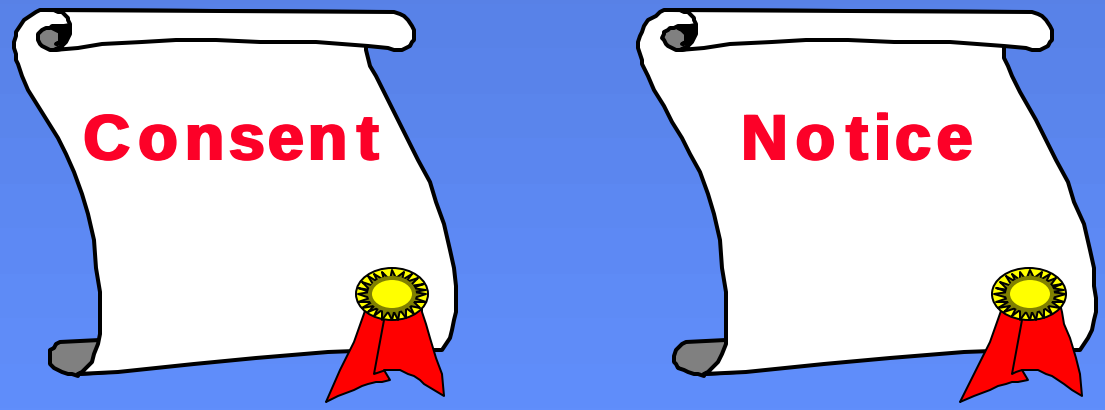
Providers can condition treatment on obtaining consent.

"Use & disclosure" is allowed for treatment, payment, and **health care operations** .... if you [the provider] have a consent signed that says so !!

# Consents: *Who, What, Where, When & How.*

May NOT be combined with a Notice a CE must provide to individuals under 164.520.

Two (2) documents required.



# Consents : *Exceptions*

## Table A-19

- Indirect treatment relationship
- Inmates
- Emergency Treatment *(must attempt to obtain consent "as soon as reasonably practicable" and if unsuccessful, document such attempt & reason the attempt failed.)*
- As "required by law"
- Communication Barrier *(but tx inferred)*

# Consents: *Who, What, Where, When & How.*

Consent can be revoked to the extent it is not already relied upon.

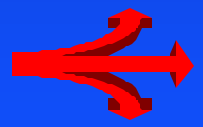
CEs must document and retain any consent obtained for six years.

Must contain required elements.

Table A-19 & A-21

# Consents: *Elements*

- Must be in plain language
- Must inform the individual that the consent allows use or disclosure for treatment, payment or health care operations.
- Must refer the individual to the NOTICE.
- Must state that the individual has a right to review the NOTICE before signing the consent.



# Consents: *Elements*
## *(continued)*

- Must describe how the individual may obtain revised notice is the CE reserved the right to revise its privacy practices.
- Must state the individual has the right to request restrictions on use & disclosure but the CE need not agree to be bound.
- Must state the individual has right to revoke the consent if not already relied upon.
- Must be dated and signed by the individual.

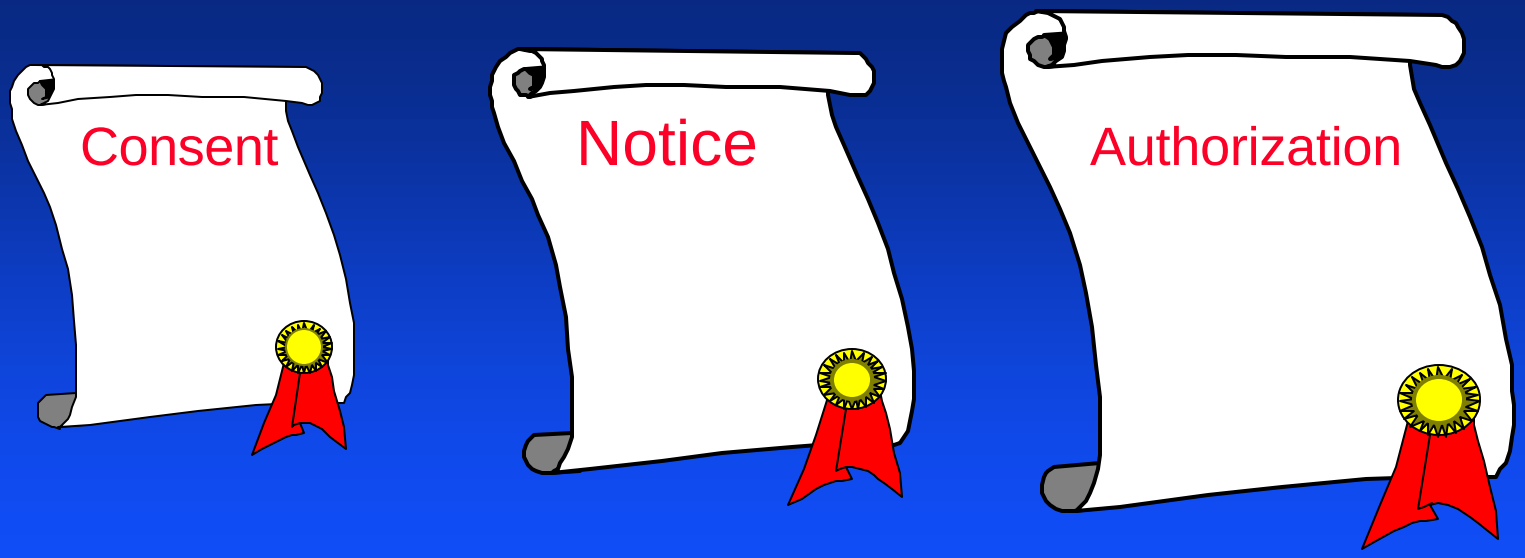
# Consents: *How many?*

Each CE is required to obtain its own consent. *(Unless the CEs participate in an organized health care arrangement.)*

If a joint consent is used then it must state the name or other specific identification of the CEs or class of CEs to which the joint consent applies.

# Consents .....

A consent is not a notice. A consent is not an authorization. And a notice is not an authorization.



# HIPAA: Day 2

Thanks for coming back.

# HIPAA: Day 1 Summary

**HCFA = CMS**

http://aspe.os.dhhs.gov/adminsimp.

All medical records & other individually identifiable health information used or disclosed by a CE in any form, whether electronically, on paper, or orally, are covered by the final rule.

# Day 1 Summary

- Providers will be required to give patients a clear written explanation of how the CE may use & disclose their health information.
- CONSENT: Health care providers who see patients will be required to obtain patient consent before sharing ("using & disclosing") their PHI for treatment, payment or health care operations. *(exceptions)*

# Day 1 Summary

- Separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes.
- Patients will have the right to request restrictions on the uses & disclosures.
- In general, disclosures of PHI will be limited to the minimum necessary for the purpose of the disclosure. *(treatment exception)*

# Day 1 Summary

- The final rule requirements are “flexible and scaleable” to account for the nature of each entity’s business, and its size and resources.
- Must adopt written privacy procedures (and “criteria”) to include who has access to PHI, how it will be used within the CE, & when it will be disclosed.

# Day 1 Summary

- BUSINESS ASSOCIATES: If an outside person is going to use PHI on your "behalf" then you must have a business associate contract (BAC).
- BAC is basically a confidentiality agreement covering uses & disclosures.
- Must monitor the BA and the BAC.

# Day 1 Summary

- NOTICE: A notice must be provided to the patient on the first day of service that explains the patient's rights, the legal duties the CE has, and what you may do with the PHI.
- The NOTICE must include examples specific to your own setting.

# Day 1 Summary

- NOTICE must be provided to the patient.
- CONSENT must refer the patient to the NOTICE & state the patient can review the NOTICE before signing, and document & retain the signed consent. (*available upon request*)
- AUTHORIZATION must be dated & signed AND provide a copy to the patient.

# Day 1 Summary

- NOTICES can be given out to each & every patient *(big document = big job).*
- NOTICES must be written but the preamble addresses people who can't read == audio & different languages.
- Restrictions must be in writing and either agreement or disagreement should be in writing. *(short form)*

# Authorizations

45 C.F.R. 164.508

**Unless provided for in HIPAA a CE may not use or disclose PHI without a HIPAA authorization**

# AUTHORIZATIONS

# Conflicts between Consents and Authorizations

- The most restrictive consent or the most restrictive authorization controls.
- The most restrictive consent or the most restrictive authorization controls regardless of when either of them was executed.
- The most recent in time does NOT control - the most restrictive one controls.

# Two Types of Authorizations

❶ Non-psychotherapy records (*e.g. regular medical records)*

➡ Must have its own authorization form.

❷ Psychotherapy Notes

➡ Must have its own authorization form.

# Disclosure without Authorization

## (Table A-28) 45 C.F.R. 164.512

- As required by law.
- For public health reporting.
- To report abuse, neglect or domestic violence.
- For health oversight.
- Judicial / Administrative proceedings.
- Cadaveric donation.
- Research purposes.
- Avert serious threat to health or safety of a person.
- Military / Veterans activities
- Workers Comp.
- Wound Reporting.
- Court / Administrative Orders Warrants.
- Law Enforcement Purpose.
- Emergency Care not on premises.
- Coroners / Funeral Directors.
- National Security & Intelligence activities.
- Protective Services for the President
- Medical Suitability.
- Correctional Institutions.
- Public benefit programs.

# Disclosure without Authorization

## *"Required by Law"* (Table A-30) 45 C.F.R. 164.514(a)

- A **mandate** (separate law) that compels disclosure.
- Must be enforceable in a court of law.
- *Examples: Medicare Conditions of Participation, court orders & court ordered warrants, grand jury subpoenas, administrative subpoenas, or statutes that require the production of information.*

# Disclosure without Authorization

## *"Health Oversight"* (Table A-31) 45 C.F.R. 164.512(d)

- HIPAA permits a CE to release PHI to a health oversight agency both federal and state.
- Disciplinary action against a professional is considered a health oversight function.
- The Kansas Board of Healing Arts and KDHE are health oversight agencies.

# Disclosure without Authorization

- Required by law.
- Public Health Activity Reporting.
- Abuse, neglect or domestic violence.
- Health Oversight.

# Disclosure without Authorization

- Judicial or Administrative proceedings.
- Wound Reporting.
- Court Order or court-ordered warrant, court / administrative subpoena or summons.

# Disclosure without Authorization

- Law enforcement request for law enforcement purpose to locate a “suspect.”
- Law enforcement request for law enforcement purpose reference a victim of a crime.
- Suspicious death by criminal conduct.

# Disclosure without Authorization

- Release to a law enforcement official about criminal conduct on the premises.
- Emergency care NOT on the premises reported to law enforcement.
- To provide information to Coroners or funeral directors.
- To provide information for Cadaveric or organ donation.

# Disclosure without Authorization

- For Research purposes.
- To avert a serious threat to health or safety of a person or the public.
- For Military & Veterans activities.
- For national security & intelligence activities.
- For protective services for the President & others.

# Disclosure without Authorization

- For medical suitability determinations.
- For correctional institutions.
- For CEs that are government programs providing public benefits.
- To disclose for workers compensation purposes.

# Verification

45 C.F.R. 164.514(h)

Know who you are releasing the PHI to.

Must verify the IDENTITY and the AUTHORITY of the person.

(Not required for facility directories or friend/family involved in health care decisions)

# PREEMPTION

45 C.F.R. 160.203

State law provisions that are contrary to the HIPAA provisions are preempted by HIPAA.

If the state law is “more stringent” (*e.g.*, provides more protection) then the state law will control.

# PREEMPTION

"More Stringent" means:

1. with respect to use or disclosure, the law prohibits or restricts a use of disclosure in circumstances which such use or disclosure otherwise would be permitted under HIPAA unless in connection with a compliance determination by the Secretary of HHS or to the individual.

# PREEMPTION

- permits greater rights of access to or amendment of the individual's health information (but shall not preempt any state law that authorizes or prohibits disclosure of PHI about a minor to a parent, guardian, or *loco parentis*.
- about a use, disclosure, right or remedy if it provides the greater amount of information.

# PREEMPTION

4. Any law that narrows the scope or duration, expand the criteria for privacy protections, or reduce the coercive effect - all related to consents or authorizations.
5. Provides for longer retention or requires reporting of more detailed information as it relates to recordkeeping or accounting.

# PREEMPTION

- OR provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

**HIPAA establishes a federal "floor" of minimum privacy standards.**

# Administrative Requirements

45 C.F.R. 164.530

- Designate a privacy official and a contact person or office (can be the same person).
- The Privacy Official is responsible for development and implementation of policies and procedures under HIPAA.
- The contact person or office is responsible for receiving complaints under HIPAA.
- Must record the designations.

# Administrative Requirements

- **Training:** Must train all workforce members on policies & procedures as "necessary and appropriate" for the members of the workforce to carry out their function within the CE.
- Workforce training must be done by the compliance date.
- Workforce training must be done for new members within a reasonable time.
- All training must be documented.

# Administrative Requirements

- SANCTIONS AND DISCIPLINE: CEs must have & implement appropriate sanctions against workforce members who fail to comply.
- Sanctions must be documented.
- The preamble states that the CE must have policies & procedures for the application of appropriate sanctions.

# Administrative Requirements

- MITIGATION: A CE must mitigate, to the extent practicable, any harmful effect that is known to the CE of a use or disclosure of PHI in violation of its policies or procedures or HIPAA.
- This relates to “harm” caused by the CE’s workforce or by its business associate.

# Administrative Requirements

- Must refrain from intimidating or retaliatory acts.
- Cannot require an individual to waive their rights to file a complaint or any other rights as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

# Administrative Requirements

- **Policies and Procedures:** CE must implement policies & procedures with respect to PHI that are designed to comply with HIPAA.
- CE must change its policies & procedures based on changes in the law or HIPAA.
- Where the CE has stated in its notice that it reserves the right to change information practices, HIPAA allows the new practice to apply to information created before the effective date of the new practice.

# Administrative Requirements

- Policies & procedures and any other required writing under HIPAA must be maintained for 6 years (the statute of limitations period for civil penalties)..... the 6 years runs from the date of creation or the date when it last was in effect ..... whichever is longer.

# Policies & Procedures

- Uses & Disclosures.
- Minimum Necessary.
- Individual Request for Restricting.
- Notices.
- Inspection & Copying.
- Amendment or Correction.
- Accounting.
- Recordkeeping
- Administrative Requirements.
- Designation of Privacy Official & others.
- Training.
- Safeguards.
- Sanctions.
- Duty to Mitigate.
- Internal Complaint.
- Consent & Authorizations.

# Resources

- The government: HHS web site, OCR web site, ....
- Other CEs
- Professional Associations
- Vendors & Business Consultant *(ALERT)*
- Your own staff *(compliance officer / committee)*
- **Legal Counsel** *(privileged communications)*

# Thank You

**GOODELL, STRATTON,**

**EDMONDS & PALMER, L.L.P.**

515 South Kansas Ave.

Topeka, KS 66603-3999

**785-233-0593**

www.goodellstrattonlaw.com

# The End