KEN PAXTON
ATTORNEY GENERAL of TEXAS

HIPAA and Medical Privacy Laws

Sinty Chandy
Assistant Attorney General
Civil Medicaid Fraud

FOCUS ON CERTAIN Medical Records Privacy Laws

- HIPAA: Privacy Rule, Security Rule, Enforcement Rule, Breach Notification Rule
- Texas Medical Records Privacy Act, Chapter 181 Texas Health & Safety Code
- Physician-Patient Communications, Chapter 159 Texas Occupations Code
- Mental Health Records, Chapter 611 Texas Health & Safety Code

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

- The Health Insurance Portability and Accountability Act (HIPAA) 45 C.F.R. Parts 160, 162, 164
- The HIPAA Privacy Rule published in 2000 by U.S. Department of Health & Human Services (HHS)
- First set of national standards for the protection of certain health information
- 2013 adoption by HHS of Omnibus Rule: Privacy Rule, Security Rule, Enforcement Rule, Breach Notification Rule

WHAT INFORMATION DOES THE HIPAA PRIVACY RULE PROTECT?

- Protected Health Information (PHI)
- All “individually identifiable health information” held or transmitted by a “covered entity” or its “business associate” in any form or media, whether electronic, paper or oral
- Information relating to a person’s past, present or future physical or mental condition, the provision of health care to that person, or the payment for the provision of health care
- Can the information be traced back to a person?

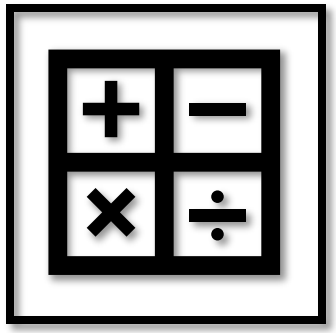
EXAMPLES OF PHI

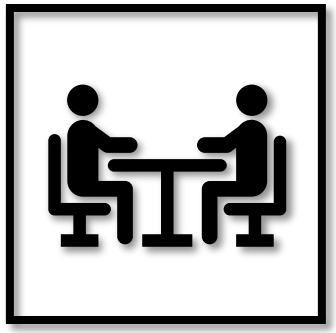
- Medical records
- Dental records
- Psychological evaluations
- Health care payments
- Lab reports

WHO MUST SAFEGUARD HIPAA PROTECTED HEALTH INFORMATION?

Covered Entities

Business Associates of Covered Entities





HIPAA COVERED ENTITIES

- Covered Entities are individuals or organizations that are subject to the HIPAA Privacy Rule
- Health Plans
- Health Care Clearinghouses
- Health Care Providers

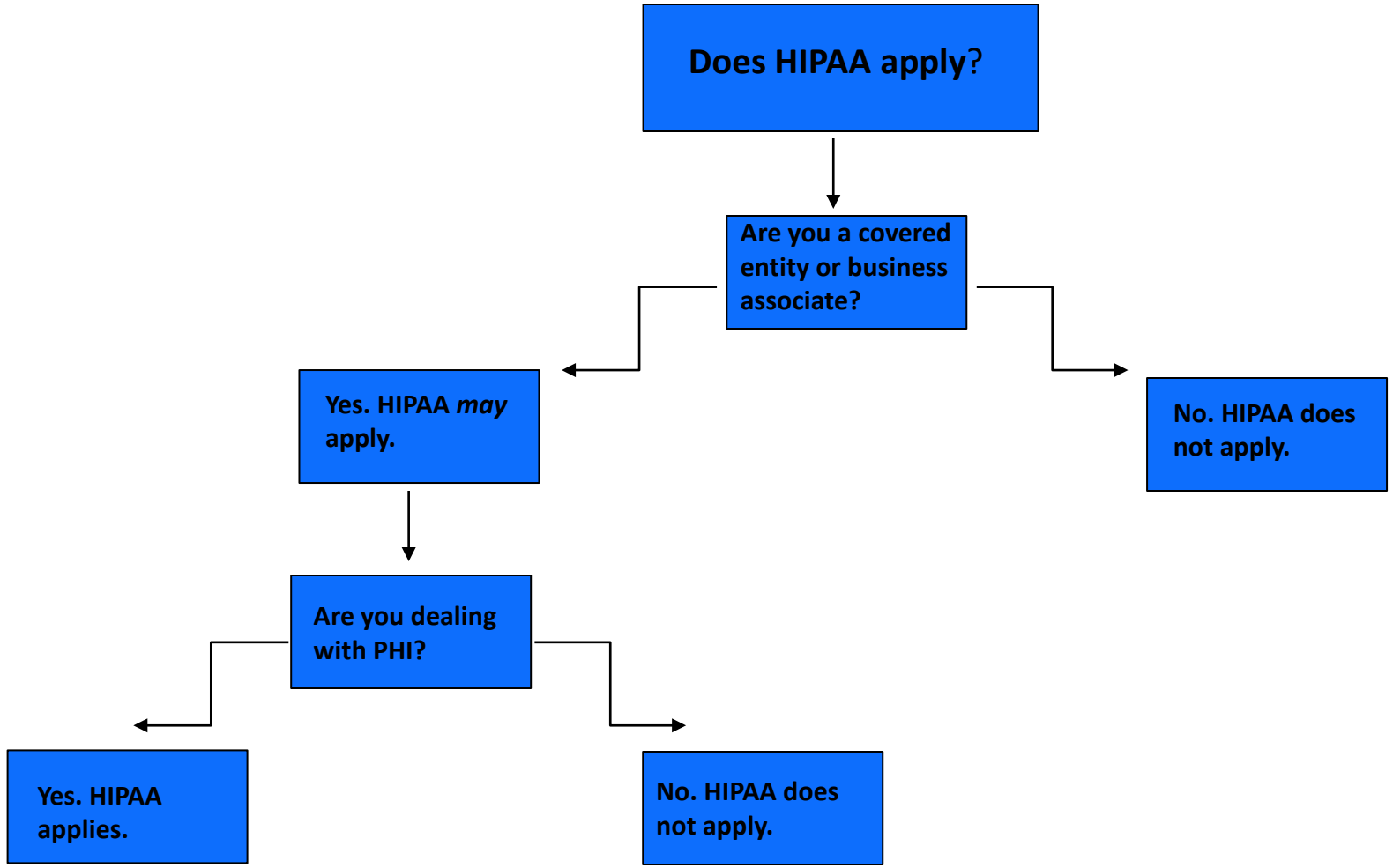
HIPAA BUSINESS ASSOCIATES

- A person or entity, outside the covered entity's workforce, performing services for the covered entity that involve the use or disclosure of PHI

- Examples: accounting, legal and consulting services

- The OAG is the business associate of state agencies that are HIPAA covered entities such as HHSC, DSHS, UTMB, etc.

DOES HIPAA APPLY?



WHO IS NOT REQUIRED TO COMPLY WITH THE HIPAA PRIVACY RULE?

- Employers
- Most state and local police or other law enforcement agencies
- Some state agencies like child protective services
- Most schools and school districts

HIPAA GENERAL RULE

- PHI may not be used or disclosed except as the HIPAA Privacy Rule permits or requires

EXAMPLES OF PERMISSIBLE DISCLOSURES UNDER HIPAA

- As required by law
- Pursuant to a written HIPAA compliant authorization
- Pursuant to a HIPAA Business Associate Agreement
- To a health oversight agency for oversight activities authorized by law
- In judicial/administrative proceedings pursuant to a HIPAA compliant protective order
- HIPAA compliant de-identification

18 IDENTIFIERS

- Names
- Geographic subdivisions smaller than a state
- All elements of date (except year)
- Telephone numbers
- Vehicle identifiers and serial numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- Social security numbers
- IP addresses
- Medical record numbers
- Biometric identifiers
- Health plan beneficiary numbers
- Full face photos
- Account numbers
- Any other unique identifying number, characteristic or code
- Certificate/license number

REMOVAL OF IDENTIFIERS

PATIENT [redacted]
DOB [redacted]
AGE 46 yrs
SEX Female
PRN [redacted]

FACILITY [redacted] M.D.
T [redacted]
F [redacted]
[redacted]

Patient identifying details and demographics

FIRST NAME	[redacted]	SEX	Female	ETHNICITY	Hispanic or Latino
MIDDLE NAME	-	DATE OF BIRTH	[redacted]		
LAST NAME	[redacted]	DATE OF DEATH	-	PREF. LANGUAGE	English
SSN	[redacted]	PRN	[redacted]	RACE	White
				STATUS	Active patient

CONTACT INFORMATION

ADDRESS LINE 1	[redacted]	CONTACT BY	Mobile Phone
		EMAIL	[redacted]
ADDRESS LINE 2	-		
CITY	[redacted]	HOME PHONE	-
STATE	[redacted]	MOBILE PHONE	[redacted]
ZIP CODE	[redacted]	OFFICE PHONE	-
		OFFICE EXTENSION	-

FAMILY INFORMATION

NEXT OF KIN	[redacted]	PATIENT'S MOTHER'S MAIDEN NAME	-
RELATION TO PATIENT	Friend		
PHONE	[redacted]	Service Date(s):	06/15/10-06/18/10
ADDRESS	- North Wilkesboro NC 28659	Account Number:	24601

HIPAA "MINIMUM NECESSARY" RULE

Even when a use or disclosure of PHI is permitted by HIPAA, only disclose the "minimum necessary" to accomplish the intended purpose of the use or disclosure.

2019 HIPAA BREACH ENFORCEMENT ACTION

- Sentara Hospitals (12 acute care hospitals with more than 300 sites throughout Virginia and North Carolina)
- Sentara mailed 577 patients' PHI to the wrong addresses.
- Sentara only reported the breach as affecting 8 individuals
- $2.175 million fine and adoption of corrective action plan that includes 2 years of monitoring

Tex. Health & Safety Code Chapter 181
TEXAS MEDICAL RECORDS PRIVACY ACT COVERED ENTITIES

- Those who for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engage in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information.

- The term “covered entity” includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site.

- **Those who come into possession of protected health information**

- Those who obtain or store protected health information

- Employees, agents, or contractors of a covered entity who creates, receives, obtains, maintains, uses, or transmits protected health information.

Tex. Occ. Code Chapter 159
PHYSICIAN-PATIENT COMMUNICATION

- “Patient” means a person who, to receive medical care, consults with or is seen by a physician

- “Medical record” does not include a billing record

- “Billing record” means a record that describes charges for services provided to a patient by a physician

WHAT INFORMATION IS PROTECTED BY TEXAS OCCUPATION CODE CHAPTER 159?

- Communications between a physician and a patient in connection with professional services rendered by the physician to the patient

- A record of the identity, diagnosis, evaluation or treatment of a patient by a physician

- Such communications and records are confidential and privileged

CAN COMMUNICATIONS AND RECORDS COVERED BY CHAPTER 159 BE DISCLOSED IN CERTAIN INSTANCES?

- The privilege of confidentiality conferred by Chapter 159 may be claimed by the patient or by the physician on behalf of the patient

- Exceptions to the privilege of confidentiality exist in certain court or administrative proceedings (list of exceptions at §159.003)

- Additional exceptions to the privilege exist (list at §159.004)

Health & Safety Code Chapter 611
MENTAL HEALTH RECORDS

- "Patient" means a person who consults with or is interviewed by a professional for diagnosis, evaluation or treatment of any mental or emotional condition or disorder, including alcoholism or drug addiction

- "Professional" means a person licensed to practice medicine in any state or nation; a person licensed or certified by Texas to diagnose, evaluate or treat any mental or emotional condition or disorder, or a person the patient reasonably believes is authorized, licensed or certified to provide such services

WHAT INFORMATION IS PROTECTED BY CHAPTER 611 TEXAS HEALTH & SAFETY CODE?

- Communications between a patient and a professional
- Records of the identity, diagnosis, evaluation or treatment of a patient that are created or maintained by a professional
- Such communications and records are confidential and privileged

CAN COMMUNICATIONS AND RECORDS COVERED BY CHAPTER 611 BE DISCLOSED IN CERTAIN SITUATIONS?

- The privilege of confidentiality may be claimed by the patient, certain persons acting on behalf of the patient and a professional acting on behalf of the patient
- Exceptions which allow disclosure exist in 11 specific circumstances (list at § 611.004)

HOW TO RECONCILE DIFFERING PROVISIONS OF MEDICAL PRIVACY LAWS

- General rule: HIPAA Privacy Rule preempts a contrary state law that provides less stringent privacy protections

CAUTION: RECOGNIZING INFORMATION COVERED BY MEDICAL PRIVACY LAWS

- Identifies an individual
- Related to health
- Documents evaluation, testing, diagnosis, treatment, consultation
- Examples: Psychotherapy notes, medical history, X-rays, test results, dental records, etc.

PRACTICAL TIPS IN LITIGATION

- Seek agreement to enter a protective order as soon as possible in a case in which use of sensitive personal information is foreseeable
- Sanitize pleadings to avoid inadvertent disclosure of sensitive personal information
- HIPAA provides two de-identification methods: 1) a formal determination by a qualified expert; or 2) the removal of specified individual identifiers, plus the absence of actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual.
- 18 specific individual identifiers must be removed
- Information may be useless after HIPAA de-identification
- File documents with the court under seal, if necessary

TAKEAWAY MESSAGE

- Golden Rule: Think about how you would want the information treated if it were your information