# Texas Medical Records Privacy Act and HIPAA and Practical Compliance Considerations

**Chris McKinney**
Orgain Bell & Tucker, LLP

Prepared for
Texas Association of Defense Counsel
2014 Summer Seminar
Coeur d'Alene, Idaho
July 16-20, 2014

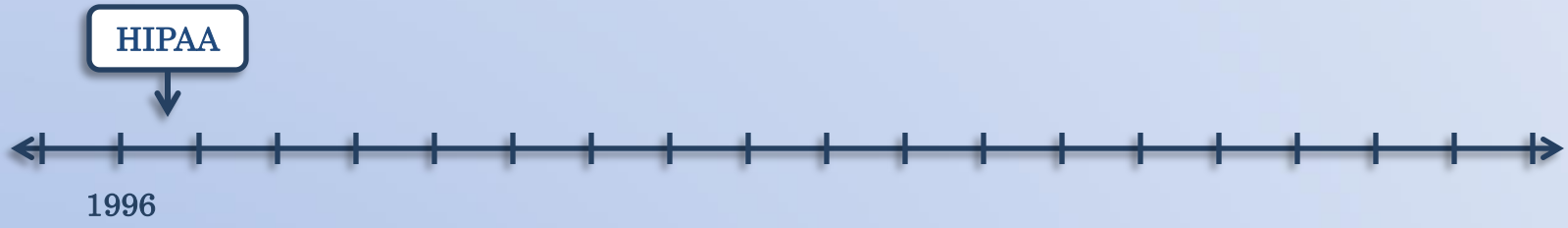
OBT
SINCE 1907

# Common Reactions

- HIPAA, schmipaa…that's for doctors. They make more money anyway.
- Great. More government regulations. You know, the founding fathers would roll over in their graves…
- What the !&%$# is House Bill 300?

OBT
SINCE 1907

# Health Insurance Portability and Accountability Act of 1996

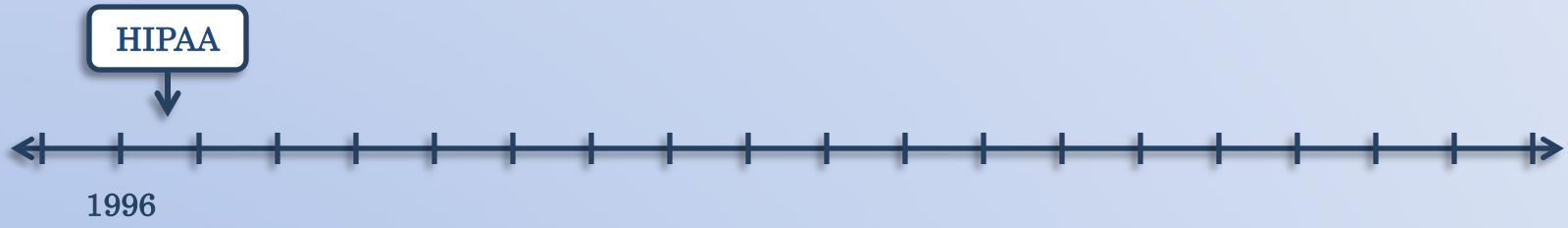



## HIPAA

Mandated that the Secretary of Health and Human Services would issue privacy regulations governing use and disclosure of "protected health information" by "covered entities."

OBT
SINCE 1907

# Health Insurance Portability and Accountability Act of 1996



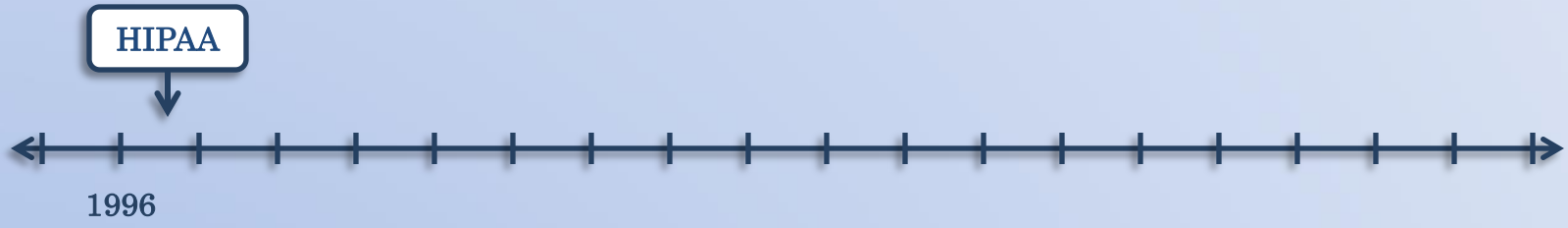

## What is "protected health information"?

Information, including demographic data, that relates to:

- The individual's past, present or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual.

OBT
SINCE 1907

# Health Insurance Portability and Accountability Act of 1996




## What are HIPAA "covered entities"?

- Health plans
- Health care providers
- Health care clearing houses

(not lawyers)

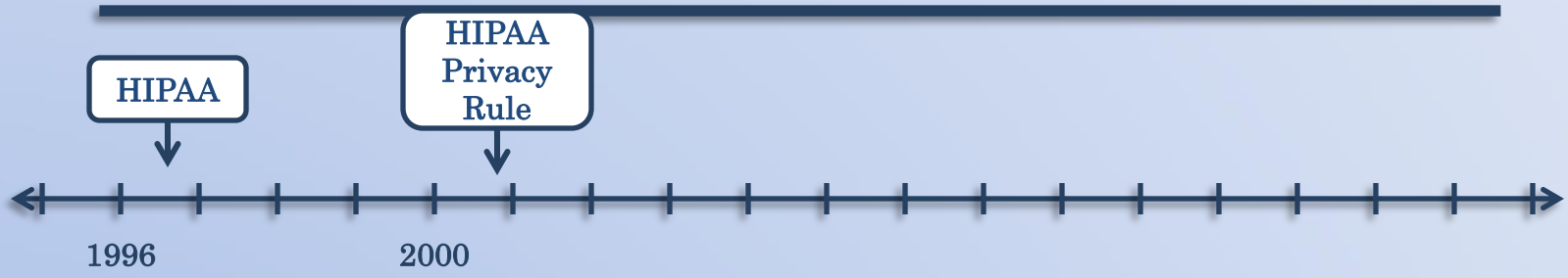
OBT
SINCE 1907

What do you call a hippo
who thinks she's sick?

A hippo-chondriac.

OBT
SINCE 1907

# HIPAA Privacy Rule



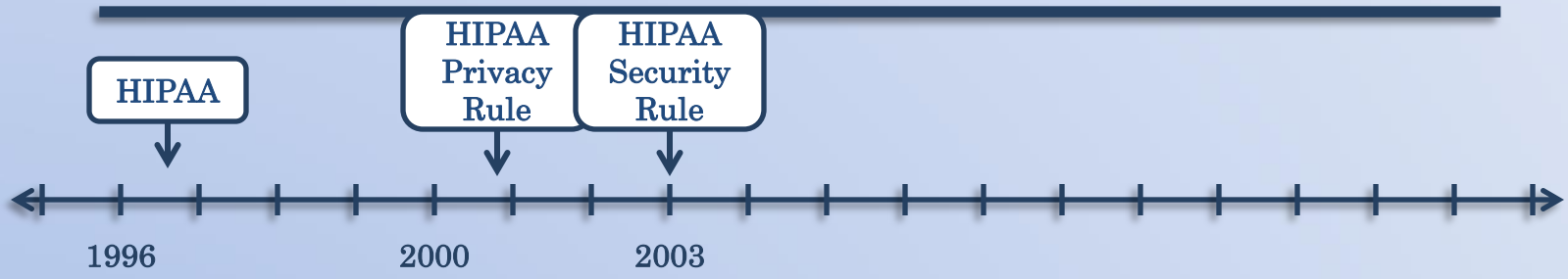

## Privacy Rule

Prohibited unauthorized disclosure of PHI.

Applied only to HIPAA "covered entities."

OBT
SINCE 1907

# HIPAA Security Rule



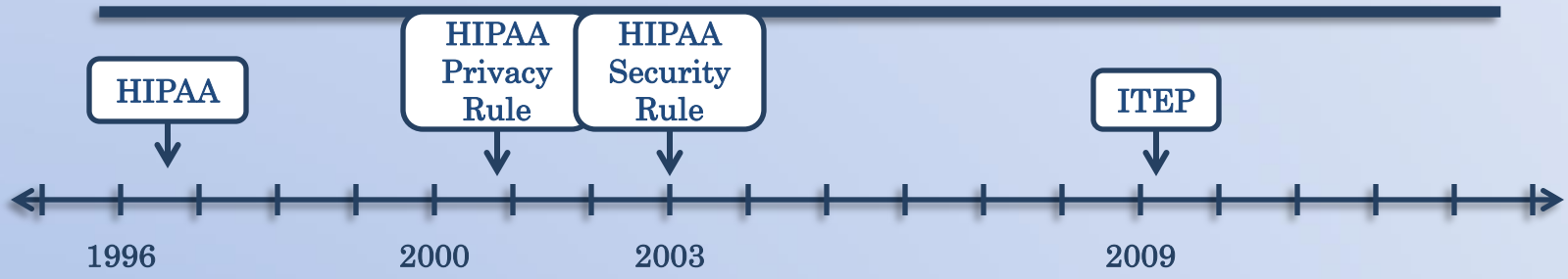

## Security Rule

Protected the integrity, confidentiality, and availability of electronic protected health information (e-PHI).

Applied only to HIPAA "covered entities."

OBT
SINCE 1907

# Texas Identity Theft Enforcement and Protection Act

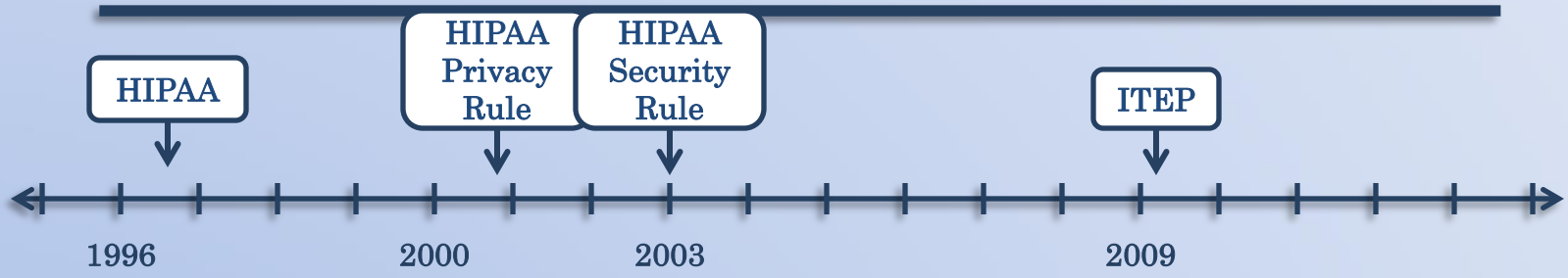



## ITEP

- Passed by Texas legislature in 2007, effective April 1, 2009
- Chapter 521 of the Texas Business &Commerce Code
- Protected "sensitive personal information" (SPI)

OBT
SINCE 1907

# Texas Identity Theft Enforcement and Protection Act



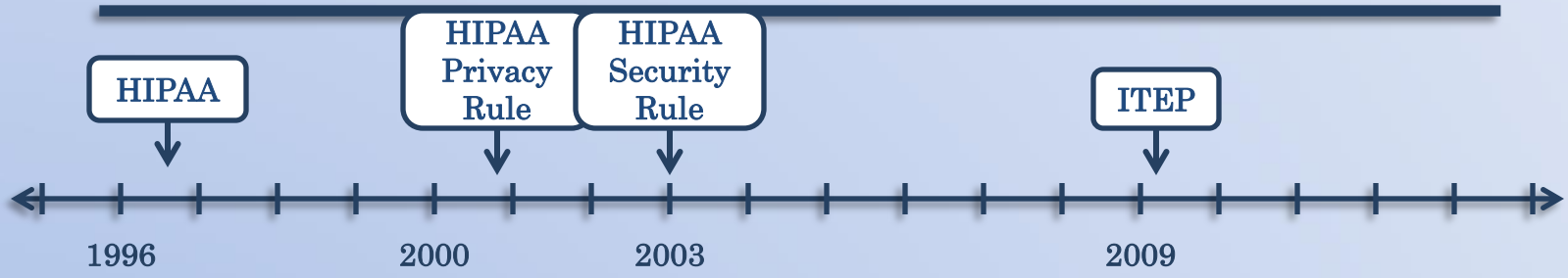

"Sensitive personal information" (SPI) means:

(A) An individual's first name or first initial and last name, in combination with any one or more of the following, if not encrypted:

- Social Security number
- Driver's license number
- Financial information

OBT
SINCE 1907

# Texas Identity Theft Enforcement and Protection Act



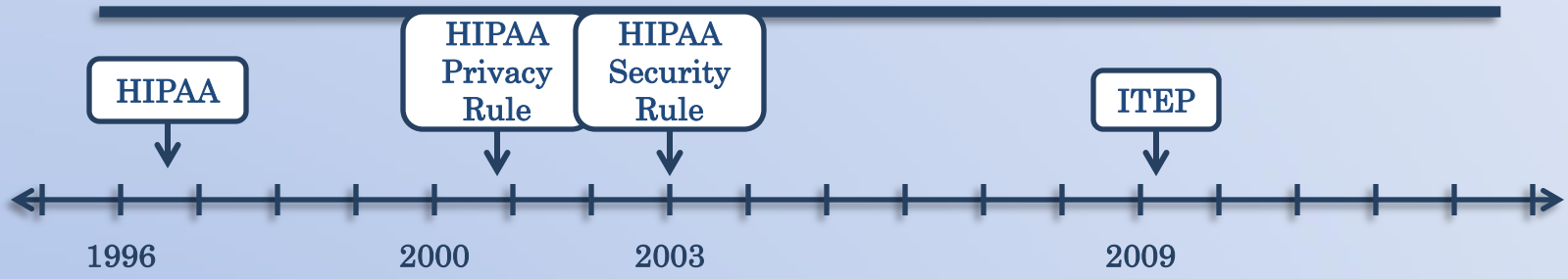

**<u>"Sensitive personal information" means:</u>**

**(B) Information that identifies an individual and relates to:**

- The physical or mental health or condition of the individual;
- The provision of health care to the individual; or
- Payment for the provision of health care to the individual.

OBT
SINCE 1907

# Texas Identity Theft Enforcement and Protection Act

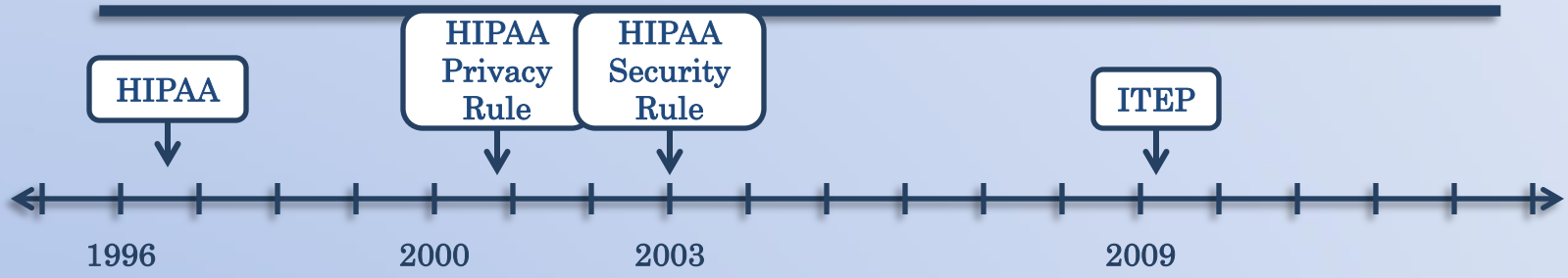



## Business Duty to Protect Sensitive Personal Information

(a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure of any sensitive personal information collected or maintained by the business in the regular course of business.

OBT
SINCE 1907

# Texas Identity Theft Enforcement and Protection Act



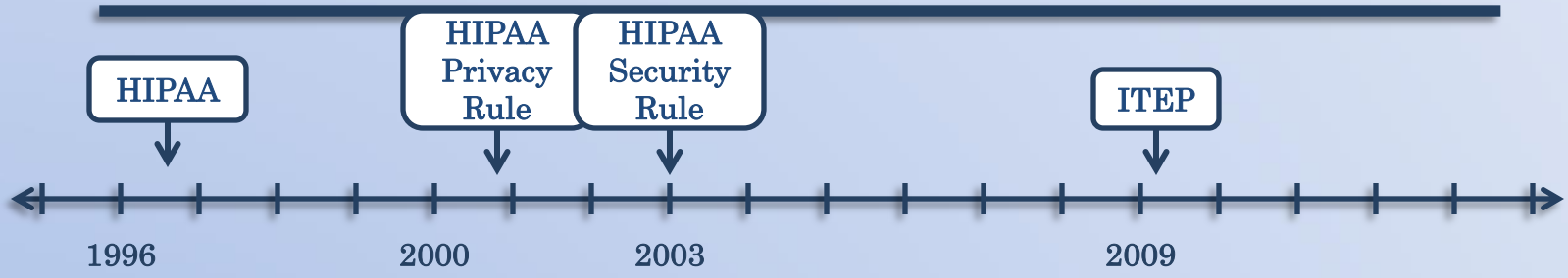

## Business Duty to Protect Sensitive Personal Information

(b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

(1) Shredding;
(2) Erasing; or
(3) Otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means.

OBT
SINCE 1907

# Texas Identity Theft Enforcement and Protection Act




## Notification Required Following Breach of Security of Computerized Data

- "Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information.
- Must provide notice of the breach as quickly as possible, pursuant to methods outlined in statute.

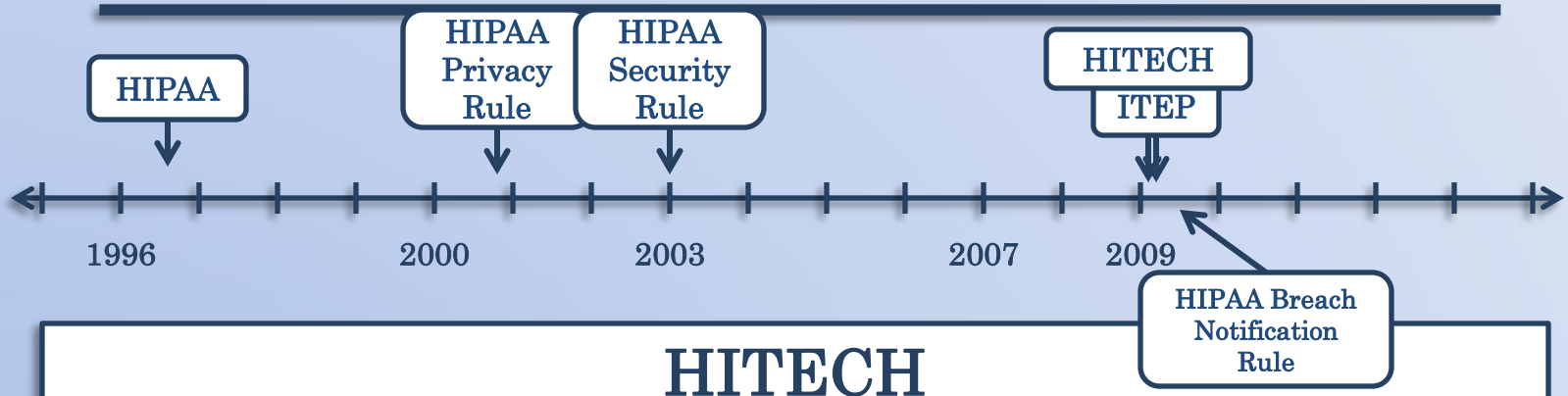
OBT
SINCE 1907

What do you call an insincere hippo?

A hippo-crite.

OBT
SINCE 1907

# Health Information Technology for Economic and Clinical Health Act

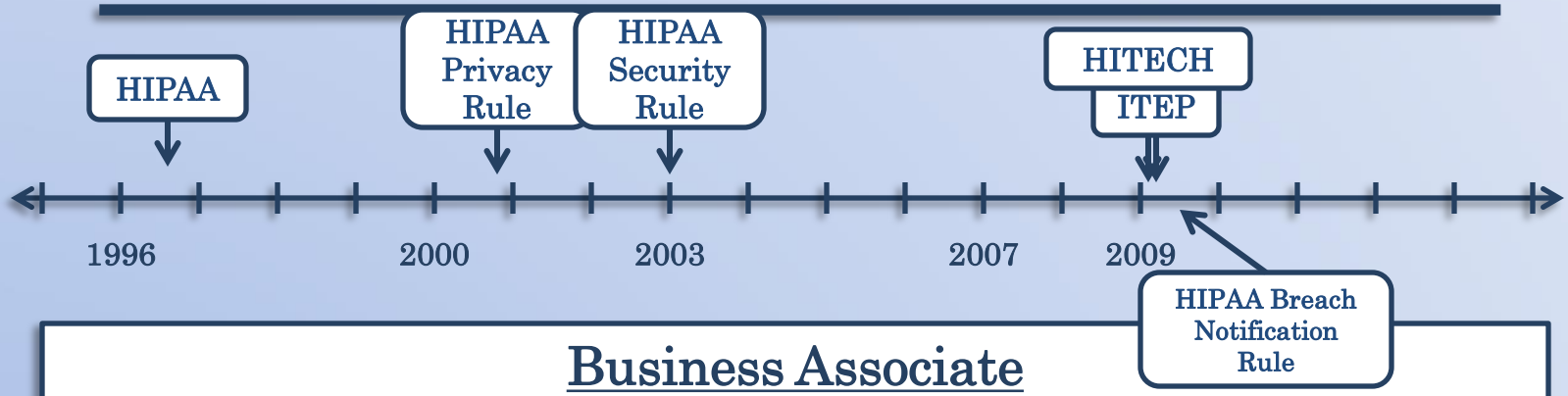



## HITECH

- Passed by Congress in early 2009, as part of stimulus bill.
- Extended HIPAA Privacy Rule and Security Rule to "business associates."
- Called for implementation of HIPAA Breach Notification Rule, which was released by HHS in August of 2009.

OBT
SINCE 1907

# Health Information Technology for Economic and Clinical Health Act

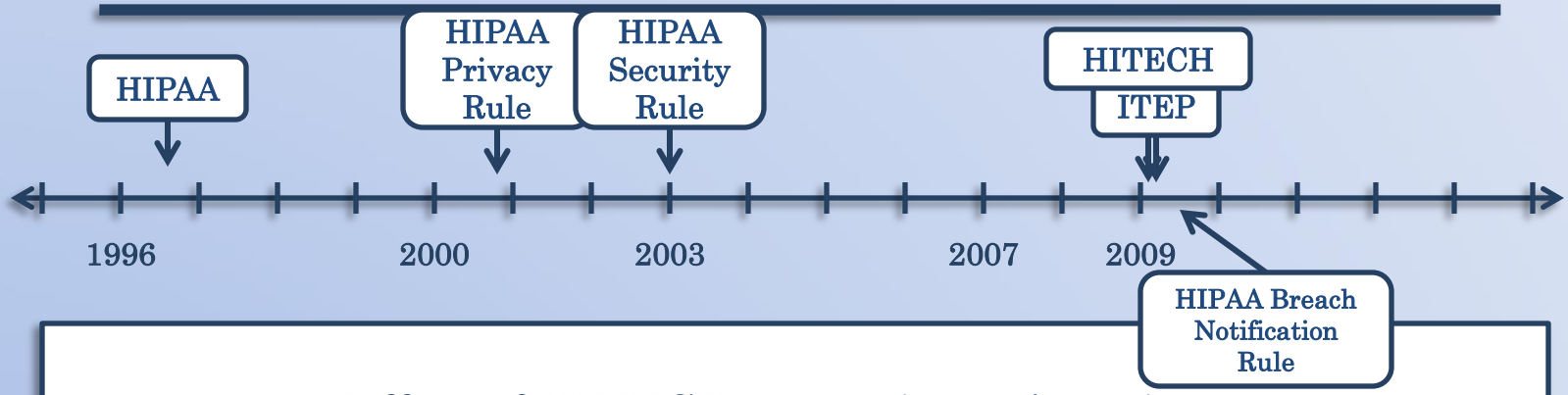



## Business Associate

- A person or organization that performs certain functions or activities on behalf of a covered entity that involve the use or disclosure of PHI.
- Legal services are specifically identified as services that may be provided by a "business associate."

OBT
SINCE 1907

# Health Information Technology for Economic and Clinical Health Act

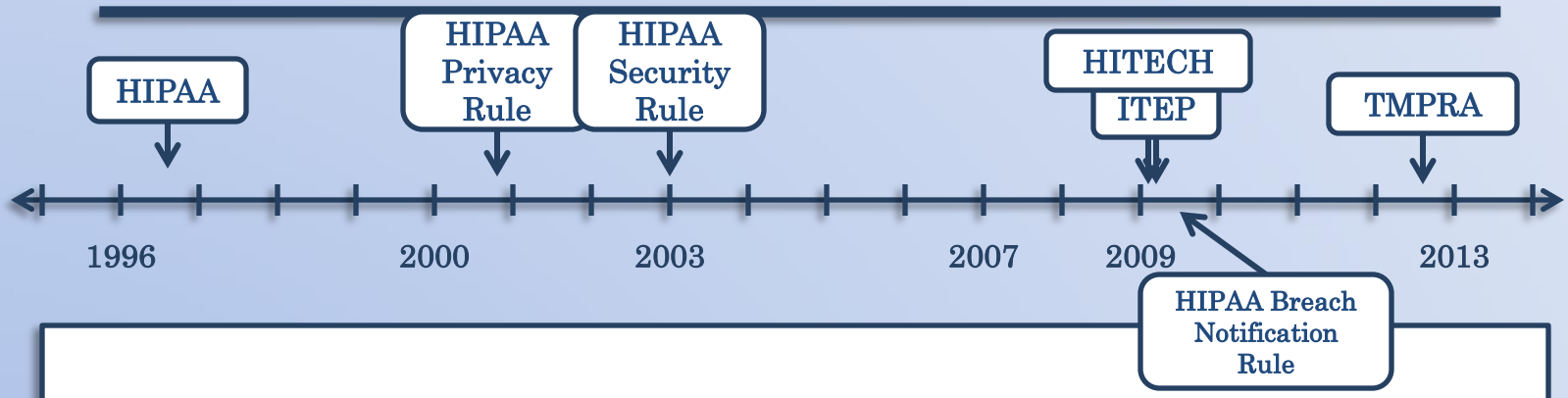



## Effect of HITECH on Business Associates

- Privacy Rule: No unauthorized disclosure of PHI.
- Security Rule: Must take affirmative steps to protect e-PHI.
- Breach Notification Rule: Must provide notice of disclosure of unprotected PHI.

OBT
SINCE 1907

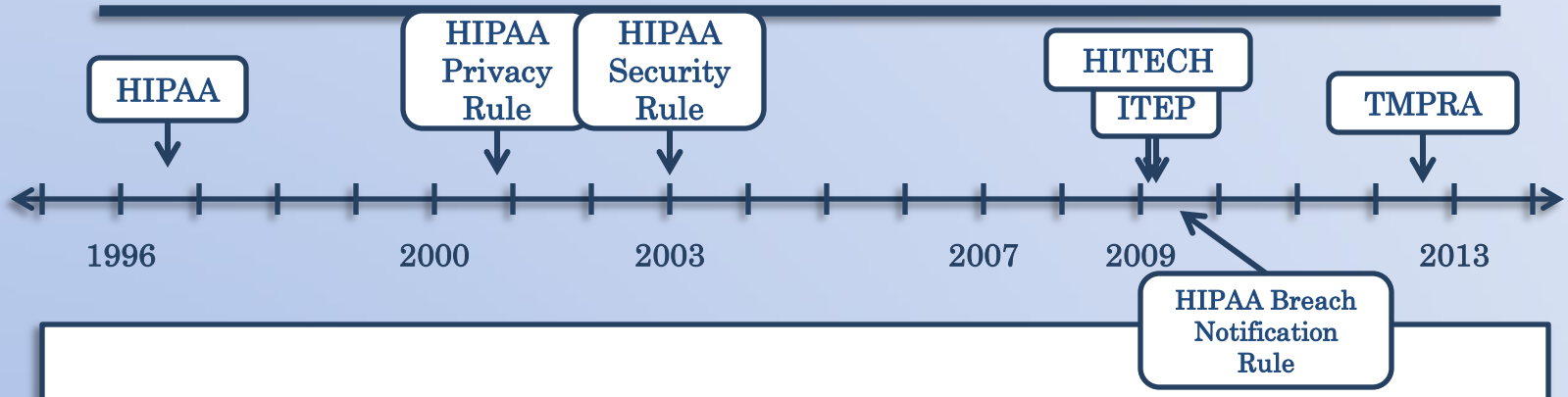
# Texas Medical Records Privacy Act




- Passed by Texas legislature on June 17, 2011.
- Effective September 1, 2012.
- Chapter 181 of the Texas Health & Safety Code.

OBT
SINCE 1907

# Texas Medical Records Privacy Act



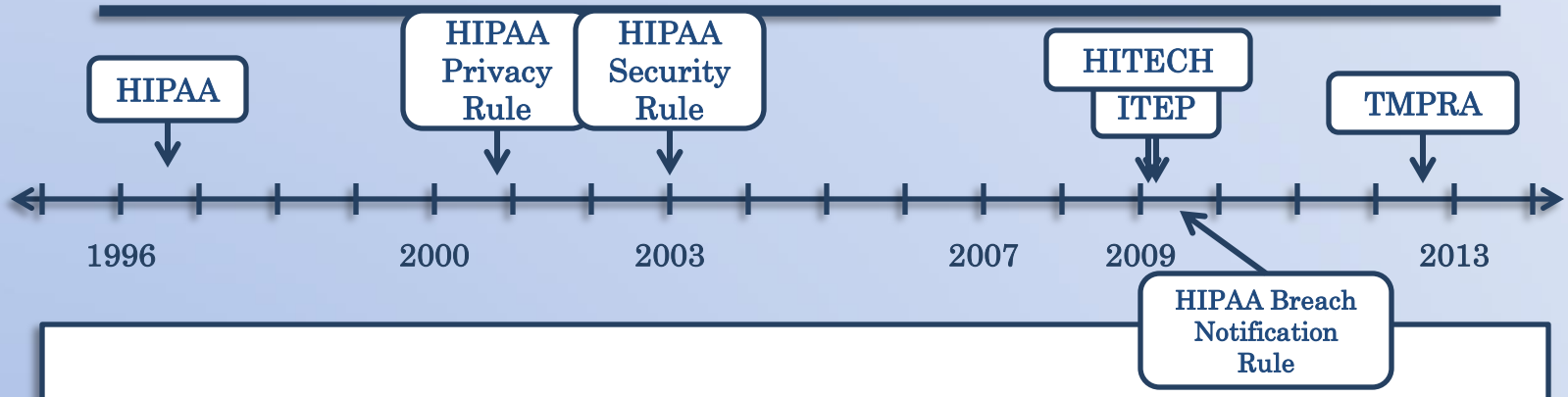

## Expanded definition of "covered entity"

"Any person who…comes into possession of protected health information"

Tex. Health & Safety Code § 181.001(b)(2)(B).

OBT
SINCE 1907

# Texas Medical Records Privacy Act



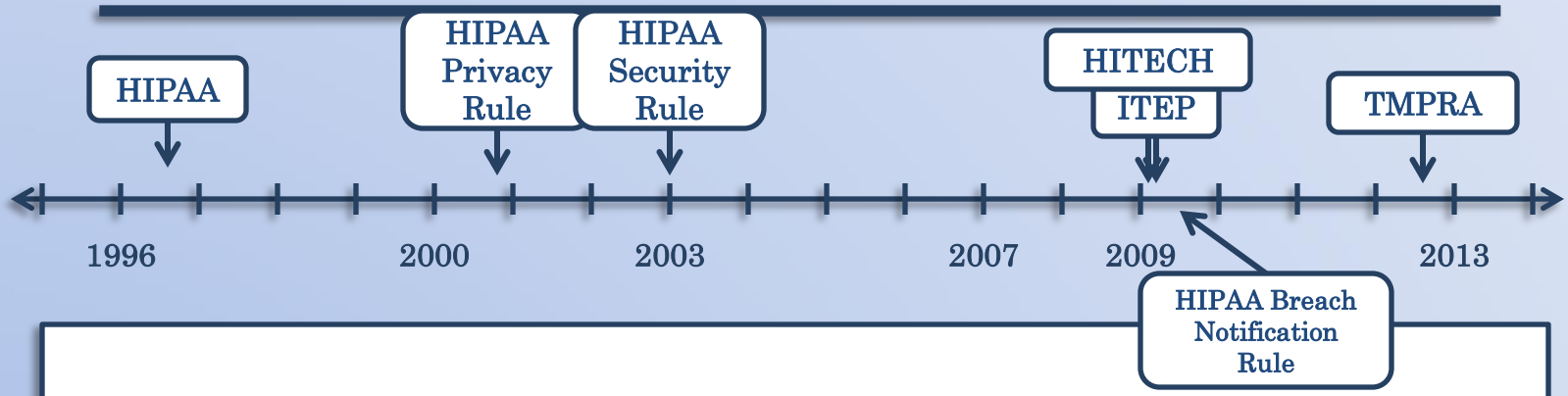

## Notice and Authorization for Electronic Disclosure of PHI

"…a covered entity may not electronically disclose an individual's protected health information without a separate authorization from the individual or the individual's legally authorized representative for each disclosure."

Tex. Health & Safety Code § 181.154(b).

OBT
SINCE 1907

# Texas Medical Records Privacy Act



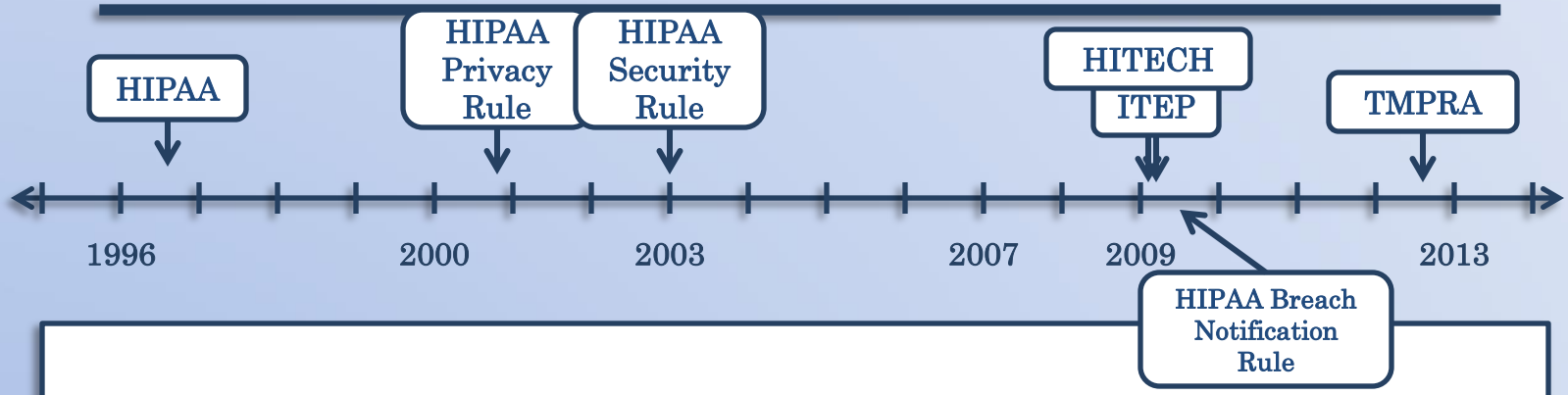

## Notice and Authorization for Electronic Disclosure of PHI

**The authorization is not required if the disclosure is made "as otherwise authorized or required by state or federal law."**

Tex. Health & Safety Code § 181.154(c).

OBT
SINCE 1907

# Texas Medical Records Privacy Act



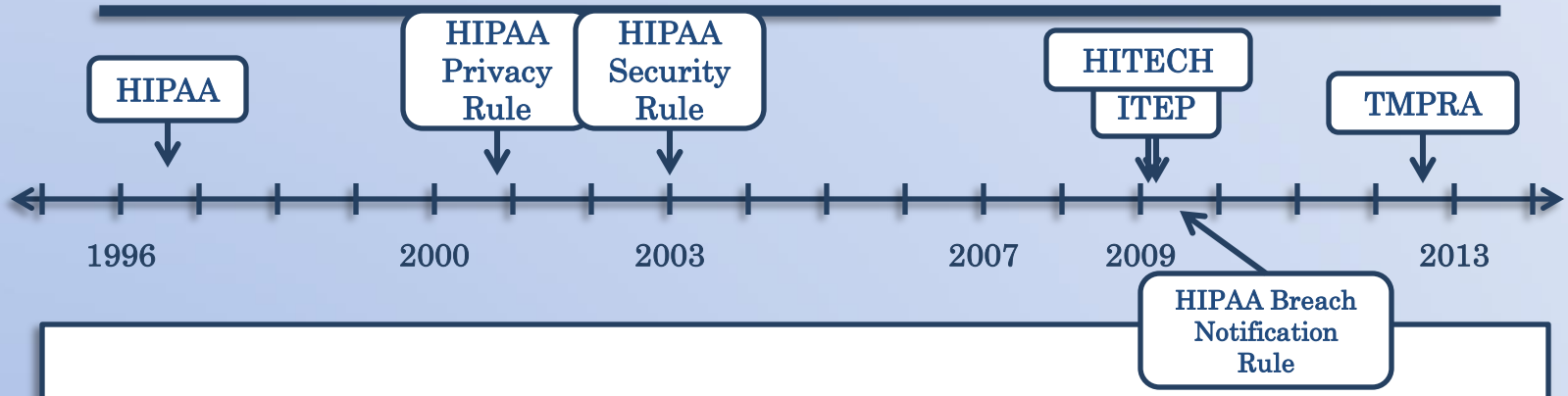

## Notice and Authorization for Electronic Disclosure of PHI

The Attorney General shall adopt a standard authorization form for use in complying with this section. The form must comply with HIPAA.

Tex. Health & Safety Code § 181.154(d).
https://www.texasattorneygeneral.gov/files/agency/hb300_auth_form.pdf

OBT
SINCE 1907

# Texas Medical Records Privacy Act




## Notice and Authorization for Electronic Disclosure of PHI

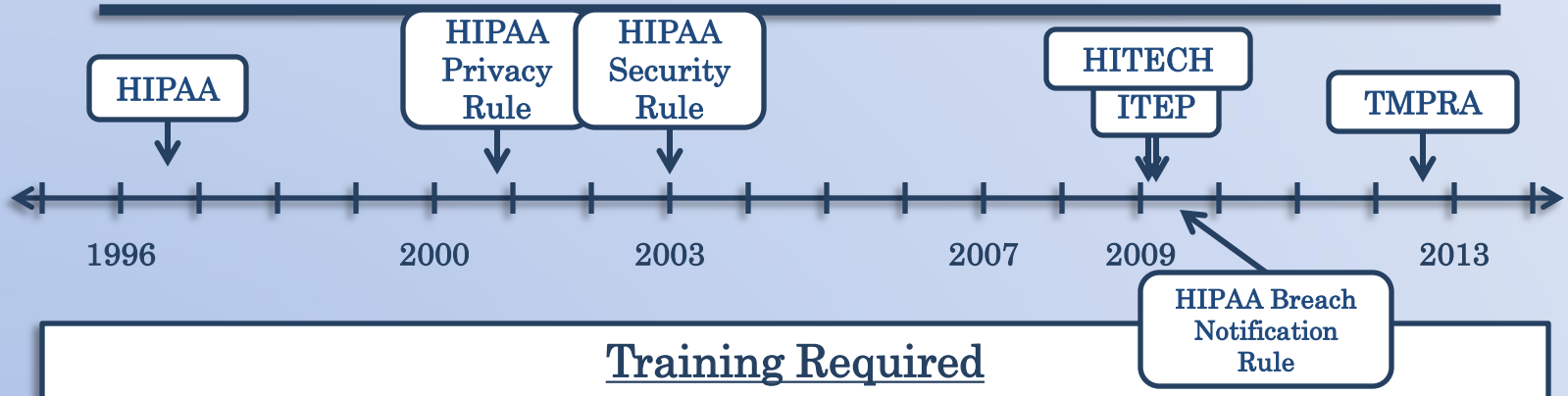
(a) A covered entity shall provide notice to an individual for whom the covered entity creates or receives protected health information if the individual's protected health information is subject to electronic disclosure. A covered entity may provide general notice by:

(1) posting a written notice in the covered entity's place of business;
(2) posting a notice on the covered entity's Internet website; or
(3) posting a notice in any other place where individuals whose protected health information is subject to electronic disclosure are likely to see the notice.

Tex. Health & Safety Code § 181.154(a).

OBT
SINCE 1907

# Texas Medical Records Privacy Act



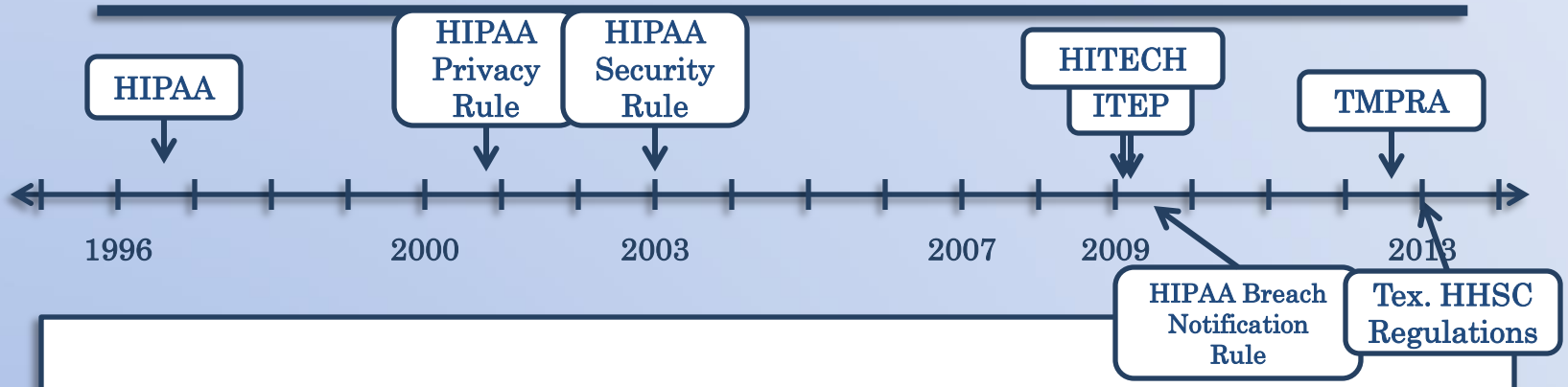

## Training Required

**(a)** Must provide training to employees regarding the state and federal law concerning PHI as necessary and appropriate for the employees to carry out the employees' duties.
**(b)** An employee's training must be completed within 90 days of hire date.
**(c)** If an employee's PHI-related job duties are materially changed by state or federal law, the employee shall receive training within a reasonable period, but not later than the first anniversary of the date the material change in law takes effect.
**(d)** An employee must sign, electronically or in writing, a statement verifying the employee's completion of training. The covered entity shall maintain the signed statement until the sixth anniversary of the date the statement is signed.

Tex. Health & Safety Code § 181.154(a).

OBT
SINCE 1907

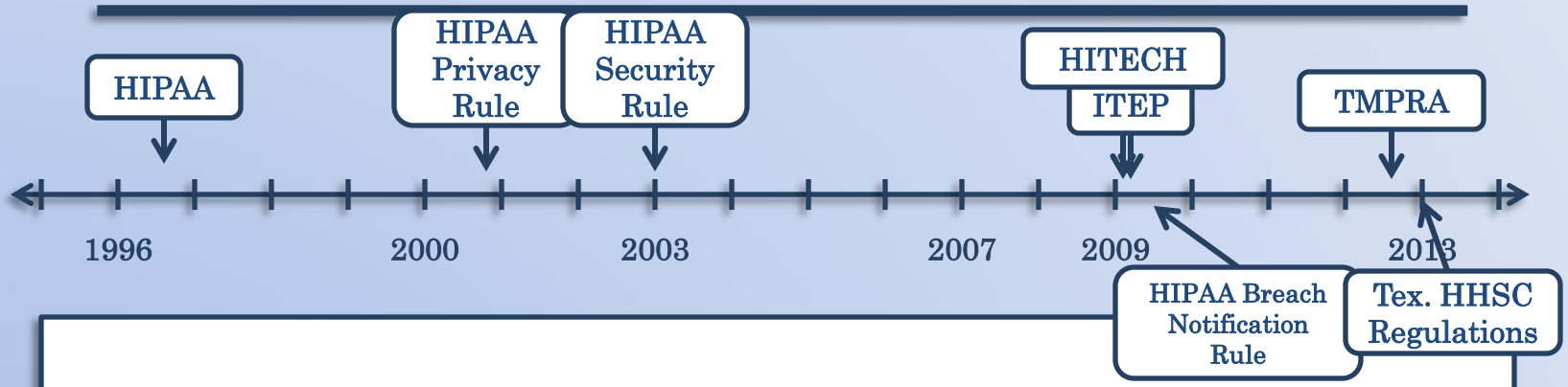
# Texas HHSC Regulations




- Implemented by HHSC pursuant to TMPRA / HB 300
- Effective January 27, 2013
- 1 Tex. Admin. Code § 390.1 – 390.2

OBT
SINCE 1907

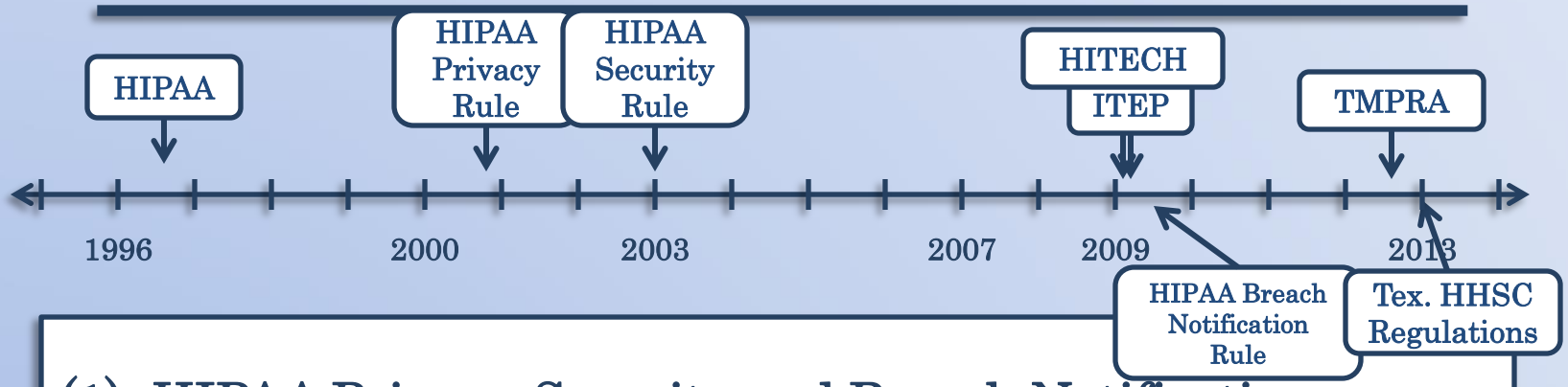
# Texas HHSC Regulations




A covered entity that electronically exchanges, uses, or discloses PHI, at a minimum, must comply with the following standards for confidential information in any form, to the extent applicable:

OBT
SINCE 1907

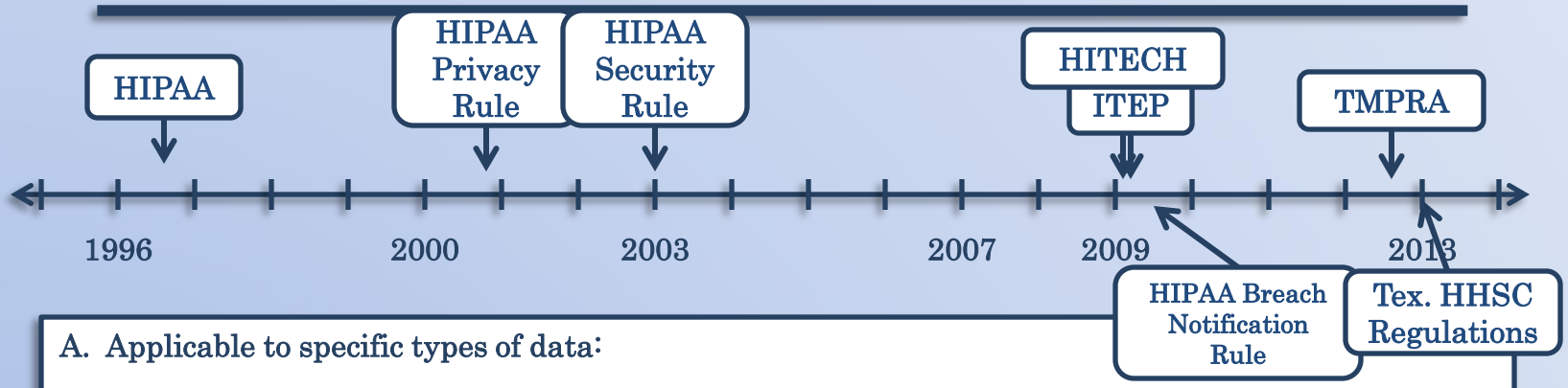
# Texas HHSC Regulations




(1) HIPAA Privacy, Security and Breach Notification Regulations;
(2) Texas Medical Records Privacy Act;
(3) Texas Identity Theft Act; and
(4) Any other applicable state or federal law or regulation that requires that confidential information be safeguarded, used, or disclosed only for authorized purposes by authorized users…

OBT
SINCE 1907

# Texas HHSC Regulations

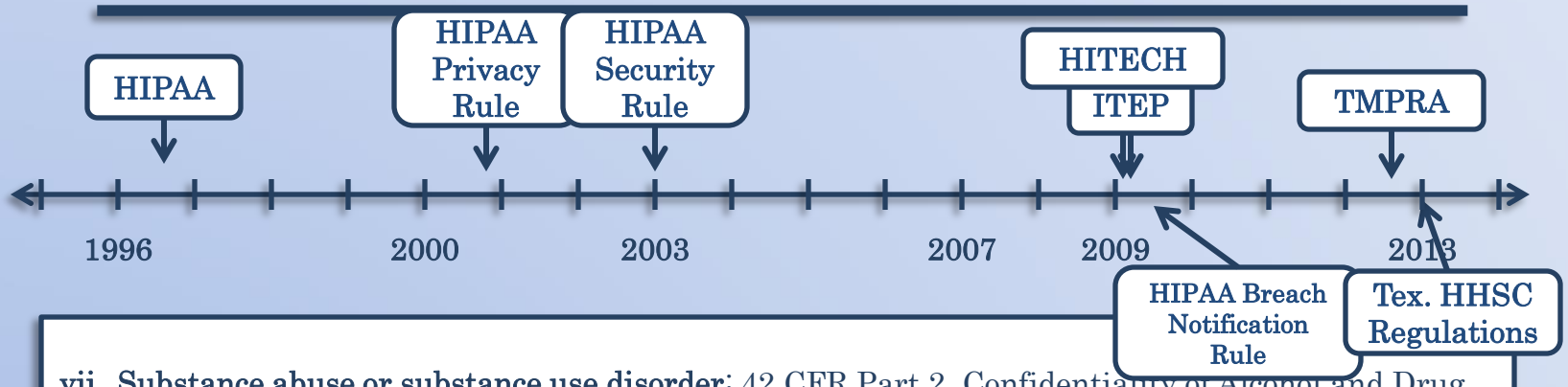



A. Applicable to specific types of data:

i. **Cancer**: Texas Health and Safety Code §82.008 and §82.009; Title 25 Texas Administrative Code (TAC) §91.9 (relating to Confidentiality and Disclosure);
ii. **HIV/AIDS**: Texas Health and Safety Code §81.103, HIV/AIDS Test Results, and 40 TAC §8.288 (relating to Confidentiality of Test Results);
iii. **Genetic**: Genetic Information Nondiscrimination Act of 2008 (GINA) Pub. L. No. 110-233 and applicable regulations promulgated under that act; Texas Insurance Code, Chapter 546, Subchapter C; Texas Labor Code §21.403 and §21.404; Texas Occupations Code, Chapter 58;
iv. **Sexual assault**: Texas Health and Safety Code, Chapter, 44, Subchapter C;
v. **Communicable diseases**: Texas Health and Safety Code §81.046; 25 TAC §97.10 (relating to Confidential Nature of Case Reporting and Records);
vi. **Mental health**: Texas Health and Safety Code, Chapter 611, Mental Health Records/Substance Abuse Records;

OBT
SINCE 1907

# Texas HHSC Regulations




vii. **Substance abuse or substance use disorder**: 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records; Texas Health and Safety Code, Chapter 611, Mental Health Records/Substance Abuse Records;

viii. **Immunizations**: Texas Health and Safety Code §161.0073 and §161.009; 25 TAC §100.2 (relating to Confidentiality);

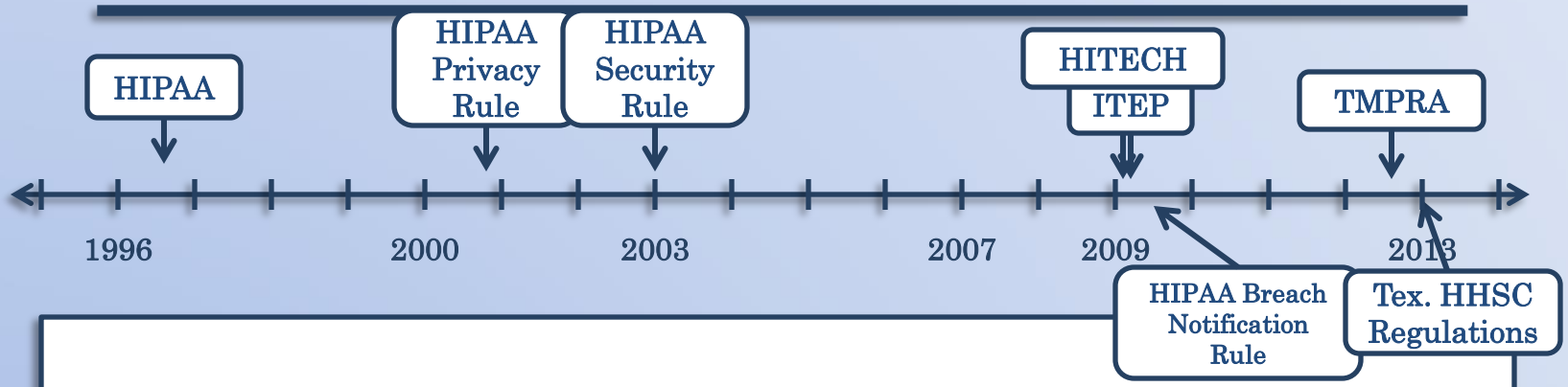
ix. **Bureau of Vital Statistics**: Texas Government Code §552.115; Texas Health and Safety Code Chapters 192 and 193, §195.005; 25 TAC Chapter 181 (relating to Vital Statistics);

x. **Reports of abuse or neglect**: Texas Human Resources Code, Chapter 48, Report of Abuse or Neglect of Elderly or Disabled Persons; Texas Health and Safety Code §161.132; Family Code Chapter 261, Reports of Child Abuse;

xi. **Federal tax information**: Internal Revenue Code, Title 26, 26 U.S.C. §6103; IRS Publication 1075;

OBT
SINCE 1907

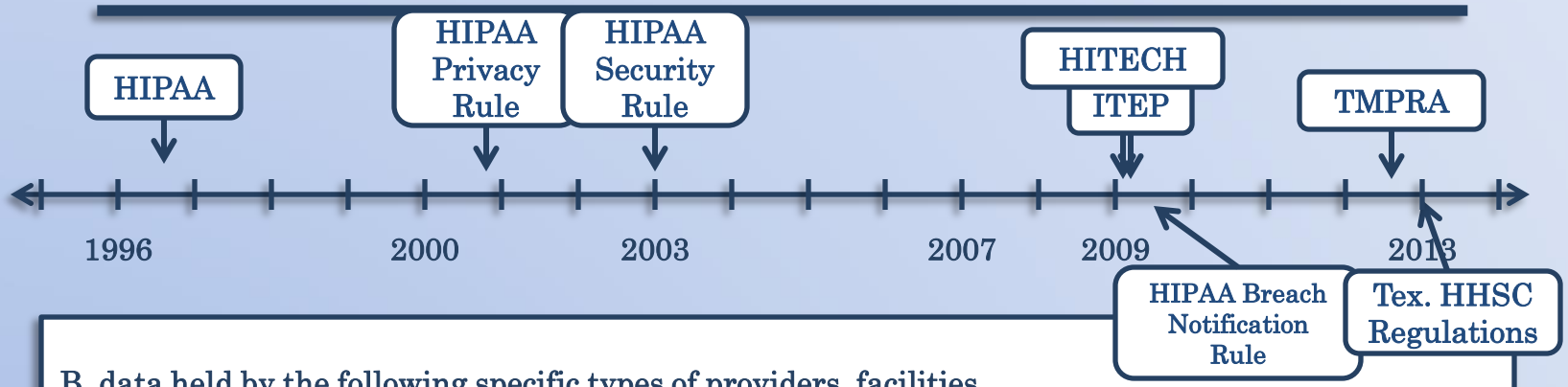
# Texas HHSC Regulations




xii. **Social Security Administration data**: 42 U.S.C. §1306, 20 CFR Part 401;
xiii. **Occupational diseases**: Texas Health and Safety Code §84.006; 25 TAC §99.1 (relating to General Provisions);
xiv. **Family planning**: 25 TAC §56.11 (relating to Confidentiality); and
xv. **Recipients of government benefits**: requirements for use of disclosure of client information about or concerning recipients of government benefits such as Medicaid, the Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance for Needy Families (TANF), or the Children's Health Insurance Program (CHIP), by HHSC or its designee(s), third party, or business associate: 7 CFR §272 (SNAP); 45 CFR §205.50 (TANF); 42 CFR §§431.300 et seq. (Medicaid); 42 CFR §457.1110 (CHIP);

OBT
SINCE 1907

# Texas HHSC Regulations

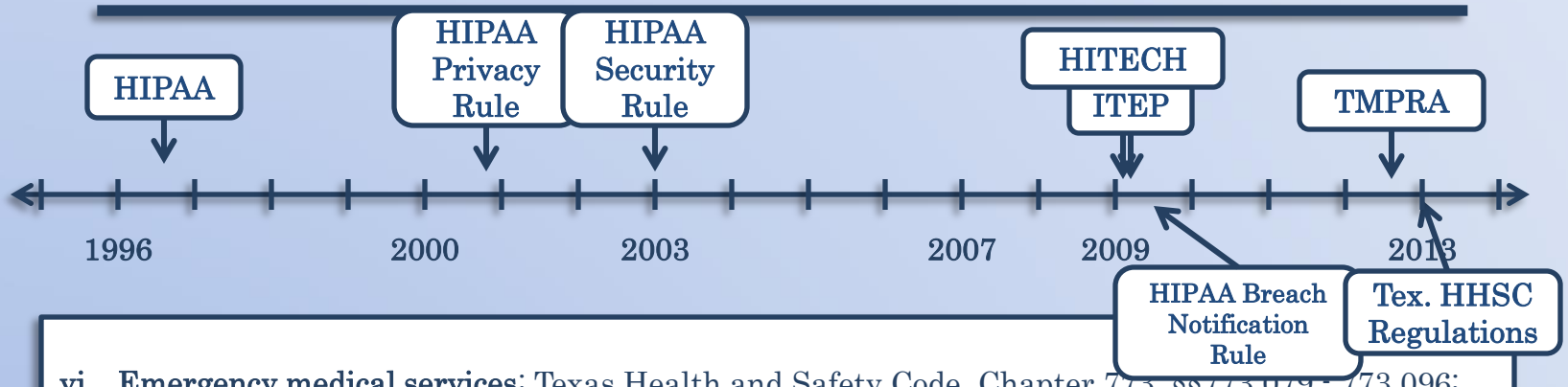



B. data held by the following specific types of providers, facilities, and services:

i. **Hospitals**: Texas Health and Safety Code, Chapter 241, Subchapter G, Hospital Disclosures of Health Care Information; 25 TAC §133.42 (relating to Patient Rights);
ii. **Nursing facilities**: Texas Health and Safety Code, Chapter 242, §242.134 and §242.501(8), Nursing Home Resident Rights; 40 TAC §19.407 (relating to Privacy and Confidentiality);
iii. **Intermediate care facilities for persons with an intellectual disability or related conditions** (ICF/IID): Texas Health and Safety Code, Chapter 252, §252.126 and §252.134;
iv. **Freestanding emergency medical care facilities**: Texas Health and Safety Code Chapter 254; 25 TAC §131.53 (relating to Medical Records);
v. **Ambulatory surgical centers**: Texas Health and Safety Code, Chapter 243, 25 TAC §135.5 (relating to Patient Rights);

OBT
SINCE 1907

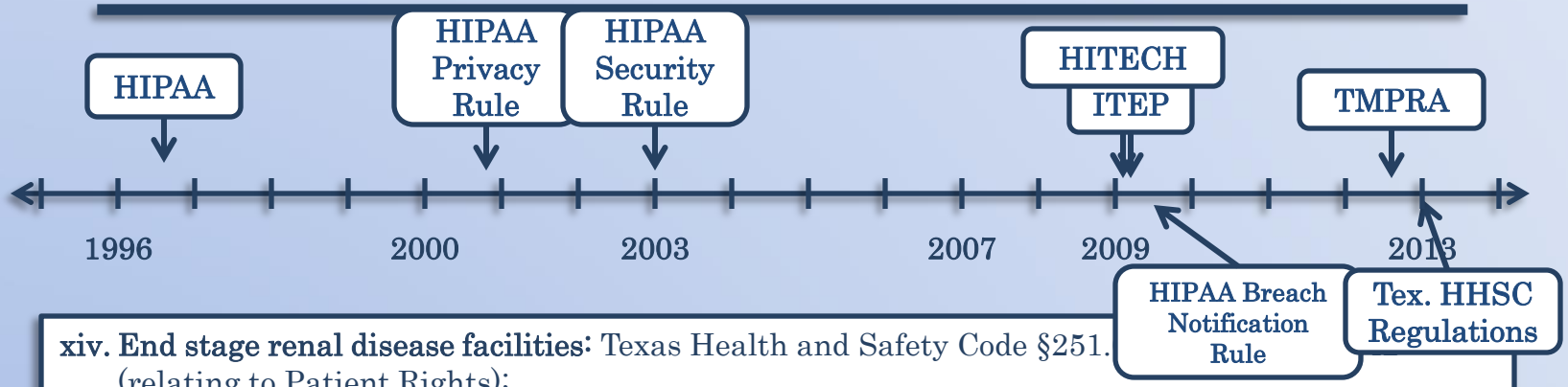
# Texas HHSC Regulations




vi. **Emergency medical services**: Texas Health and Safety Code, Chapter 773, §§773.079 - 773.096; 25 TAC §157.11 (relating to Requirements for an EMS Provider License);
vii. **Physicians**: Texas Occupations Code, Chapter 159, Physician-Patient Communication;
viii. **Chiropractors**: Texas Occupations Code §§201.402 - 201.405, Chiropractor-Patient Confidentiality;
viii. **Dentists**: Texas Occupations Code §§258.051 et seq., Dental-Patient Confidentiality;
ix. **Labs**: Clinical Laboratory Improvement Amendments (CLIA) (1988); 42 CFR §493.1291;
x. **Pharmacists**: Texas Occupations Code, Chapter 562, §562.052, Confidential Records of Pharmacists;
xi. **Podiatrists**: Texas Occupations Code, Chapter 202, Subchapter I, §§202.401 et seq., Podiatrist Privilege and Confidentiality;
xii. **Personal health record vendors**: Health Breach Notification Rule for Vendors of Personal Health Records, 16 CFR Part 318;

OBT
SINCE 1907

# Texas HHSC Regulations




xiv. **End stage renal disease facilities:** Texas Health and Safety Code §251. (relating to Patient Rights);

xv. **Special care facilities (AIDS):** 25 TAC §125.33 (relating to Resident Rights);

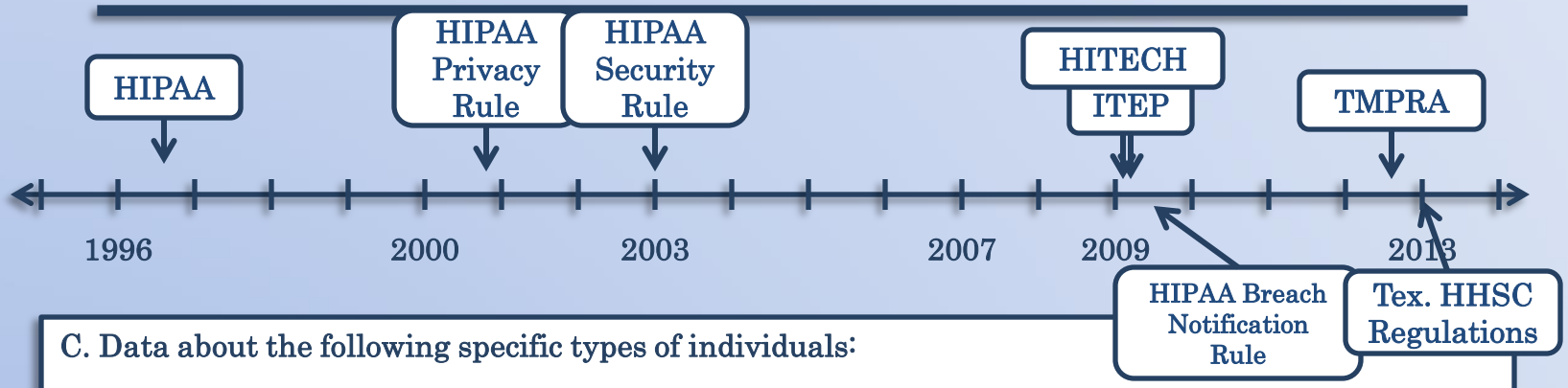
xvi. **Private psychiatric hospitals and crisis stabilization units**: Texas Health and Safety Code §577.013: 25 TAC Chapter 134 (relating to Private Psychiatric Hospitals and Crisis Stabilization Units);

xvii. **Birthing centers:** 25 TAC §137.53 (relating to Clinical Records);

xviii. Applicable health professions regulated by 25 TAC Chapter 140 (relating to Health Professions Regulation) confidentiality requirements under 25 TAC Chapter 140 or other applicable law for, such as: (I) **licensed chemical dependency counselors and treatment facilities**, Texas Occupations Code §504.251; 25 TAC §140.424 (relating to Standards for Private Practice); Texas Health and Safety Code, Chapter 464; 25 TAC Chapter 448 (relating to Standard of Care); (II) **medical radiologic technologists**, 25 TAC §140.514 (relating to Disciplinary Actions); (III) **dyslexia therapists and dyslexia practitioners**, 25 TAC §140.586 (relating to Code of Ethics; Duties and Responsibilities of License Holders); and (IV) **promotores or community health workers**: 25 TAC §146.11 (relating to Professional and Ethical Standards);

OBT
SINCE 1907

# Texas HHSC Regulations

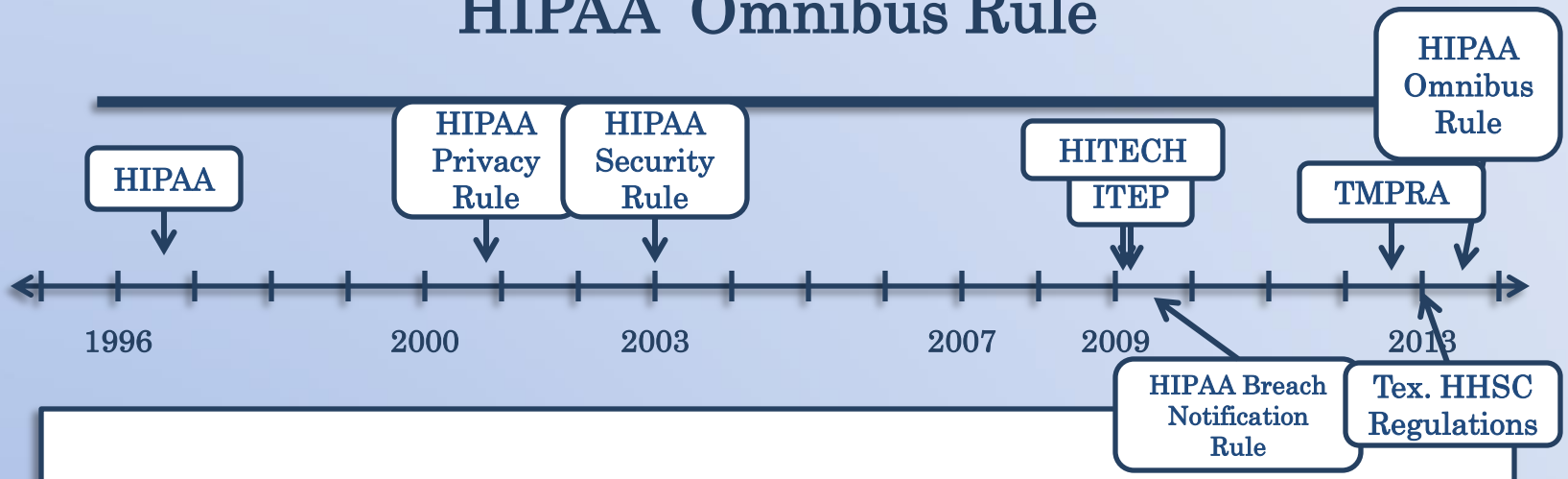



C. Data about the following specific types of individuals:

i. **Minors**: Texas Family Code §§32.003, 32.004, 151.003, 153.073, 153.074, and 153.132; Texas Occupations Code §159.005; Texas Civil Practice and Remedies Code §129.001;
ii. **Children with Special Health Care Needs Services Program**: 25 TAC §38.5 (relating to Rights and Responsibilities of a Client's Parents, Foster Parents, Guardian, or Managing Conservator, or an Adult Client); and
iii. **Early and Periodic Screening, Diagnosis, and Treatment**: 25 TAC §33.30 (relating to Confidentiality of Records).

OBT
SINCE 1907

# HIPAA Omnibus Rule




- HHS final rule modifying HIPAA privacy rule, security rule, and breach notification rule.

- Effective Date: March 26, 2013
- Compliance Date: September 23, 2013

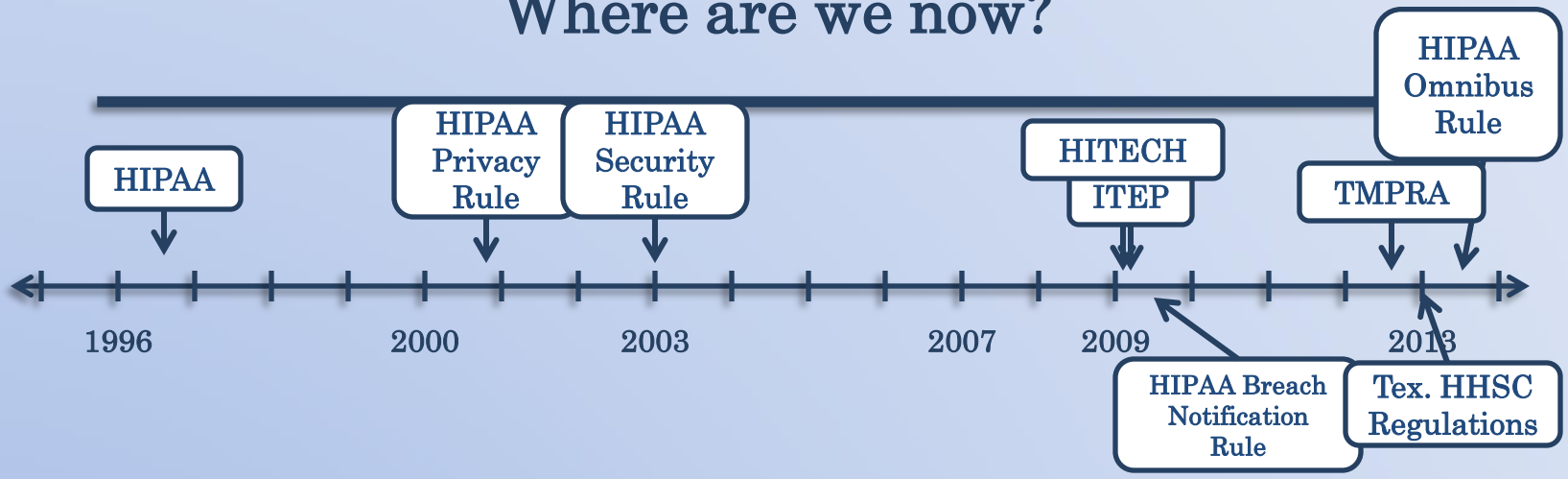
OBT
SINCE 1907

What's cool, Irish, and loves to splash in the river?

A hip O'Potamus.

OBT
SINCE 1907

# Where are we now?




In most circumstances, an attorney who uses or otherwise comes into possession of protected health information should comply with – at a minimum – the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule.

OBT
SINCE 1907

# Practical Application: Security

**General requirements of the Security Rule**

Covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

OBT
SINCE 1907

# Practical Application: Security

In most instances, the Security Rule does not dictate specific security measures. Instead, the measures should be tailored to the particular entity, considering:

- Its size, complexity, and capabilities,
- Its technical, hardware, and software infrastructure,
- The costs of security measures, and
- The likelihood and possible impact of potential risks to e-PHI.

Covered entities must review and modify their security measures to continue protecting e-PHI "in a changing environment."

OBT
SINCE 1907

# Practical Application: Security

**Security Official**

A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

OBT
SINCE 1907

# Practical Application: Security

## Risk Analysis

The Security Rule requires an entity to perform a risk analysis. The risk analysis should include (but not be limited to) the following:

- Evaluation of the likelihood and impact of potential risks to e-PHI;
- Implementation of the appropriate security measures to address identified risks;
- Documentation of chosen security measures and rationale; and
- Maintenance of continuous, reasonable, and appropriate security protections.

OBT
SINCE 1907

# Practical Application: Security

**Access Management / Role-Based Access**

A covered entity must implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role.

OBT
SINCE 1907

# Practical Application: Security

**Workforce Training and Management**

A covered entity must properly train and supervise staff who work with e-PHI.

Appropriate sanctions must be enforced against staff who violate policies and procedures.

OBT
SINCE 1907

# Practical Application: Security

**Physical Safeguards**

Must limit physical access to facilities.

Must implement policies and procedures regarding authorized access to workstations.

OBT
SINCE 1907

# Practical Application: Security

## Technology "Glitches"

- Password protection on mobile devices.
- Time-out requirements on mobile devices.
- No access to unsecured networks.
- Strong passwords.
- Expiration of passwords.
- Time-out requirements for desktops.
- Encryption of emails.
- Encryption of files.
- Limitations on file sharing.
- Destruction of electronic devices.

OBT
SINCE 1907

# Practical Application: Security

## Technical Safeguards

- **Access Control**. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).
- **Audit Controls**. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- **Integrity Controls**. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
- **Transmission Security**. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

OBT
SINCE 1907

# Practical Application: Business Associates

HIPAA requires a covered entity to have business associate agreements with all business associates.

Elements of the contract are specified at 45 C.F.R. 504(e). Generally, the agreement must describe and limit the authorized use and disclosure of PHI.

OBT
SINCE 1907

# Practical Application: Business Associates

**Who is a Business Associate?**

A business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of PHI.

OBT
SINCE 1907

# Practical Application: Business Associates

**Who is a Business Associate?**

Business associate functions include claims processing, data analysis, utilization review, and billing.

OBT
SINCE 1907

# Practical Application: Business Associates

**Who is a Business Associate?**

Business associate services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

OBT
SINCE 1907

# Practical Application: Business Associates

**Who is a Business Associate?**

Persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.

OBT
SINCE 1907

# Practical Application: Business Associates

## Who is a Business Associate?

From HHS guidance:

**US Postal Service, United Parcel Service, delivery truck line employees?**

**No,** the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.

OBT
SINCE 1907

# Practical Application: Business Associates

## Who is a Business Associate?

From HHS guidance:

**Software vendors?**

**Maybe.** The mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the protected health information of the covered entity. If the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity. For example, a software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function, is a business associate of a covered entity.

OBT
SINCE 1907

# Practical Application: Business Associates

## Who is a Business Associate?

From HHS guidance:

**Janitors?**

**No.** A business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. Generally, janitorial services that clean the offices or facilities of a covered entity are not business associates because the work they perform for covered entities does not involve the use or disclosure of protected health information, and any disclosure of protected health information to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the HIPAA Privacy Rule.

OBT
SINCE 1907

# Practical Application: Business Associates

## Who is a Business Associate?

From HHS guidance:

**Plumbers, electricians or photocopy machine repairmen who provide repair services in a covered entity's office?**

**No.** Plumbers, electricians and photocopy repair technicians do not require access to protected health information to perform their services for a physician's office, so they do not meet the definition of a "business associate." Under the HIPAA Privacy Rule, "business associates" are contractors or other non-workforce members hired to do the work of, or for, a covered entity that involves the use or disclosure of protected health information. Any disclosure of protected health information to such technicians that occurs in the performance of their duties (such as may occur walking through or working in file rooms) is limited in nature, occurs as a by-product of their duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the Privacy Rule.

OBT
SINCE 1907

# Practical Application: Business Associates

## Who is a Business Associate?

From HHS guidance:

**Shredding service?**

**Yes.** If a service is hired to do work for a covered entity where disclosure of protected health information is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), it likely would be a business associate.

OBT
SINCE 1907

# Practical Application: Disclosures in Litigation

## HIPAA: When can PHI be disclosed in litigation?

A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if

(A) The covered entity receives satisfactory assurance…from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance…from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of…this section.

OBT
SINCE 1907

# Practical Application: Disclosures in Litigation

**Practice Problems**

**What issues are likely to arise in the following situations?**

- Providing medical records to an expert.
- Disclosing protected health information to a client.
- Forwarding copies of medical records to a co-defendant.
- Filing a motion that requires disclosure of protected health information.
- Responding to a plaintiff's request for a non-party employee's personnel records or driver qualification file.
- Issuing a subpoena for protected health information without an authorization.

OBT
SINCE 1907

How can you be sure a hippo is telling you the truth?

Make him take the hippo-cratic oath.

OBT
SINCE 1907