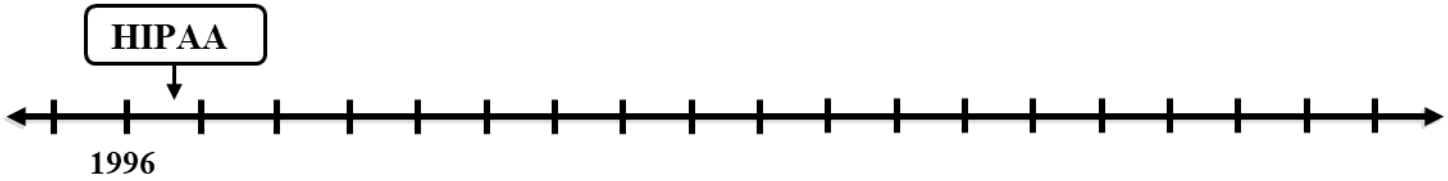
ACCREDITATION UNIVERSITY

HIPAA MARKETING GUIDELINES: HOW TO AVOID LEGAL TRAPS

Denise M. Leard, Esq.

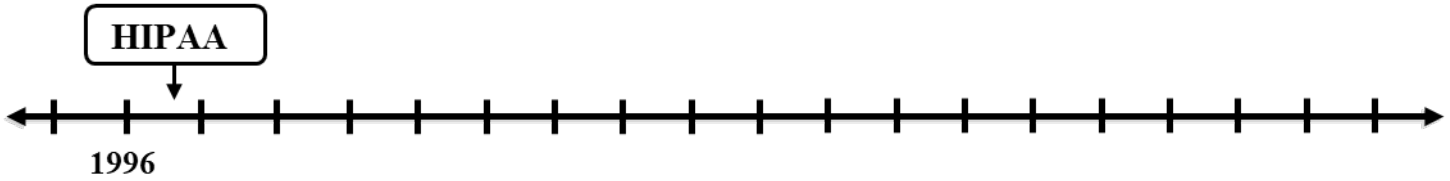
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996



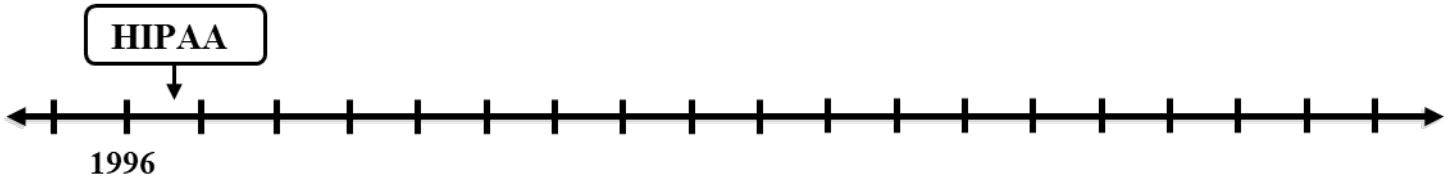
- Enacted to address privacy and security concerns with use and disclosure of “protected health information” by “covered entities”.
- Includes the “Privacy Rule” and “Security Rule”.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996



- 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.
- And identifies, or could reasonably be used to identify, the individual.

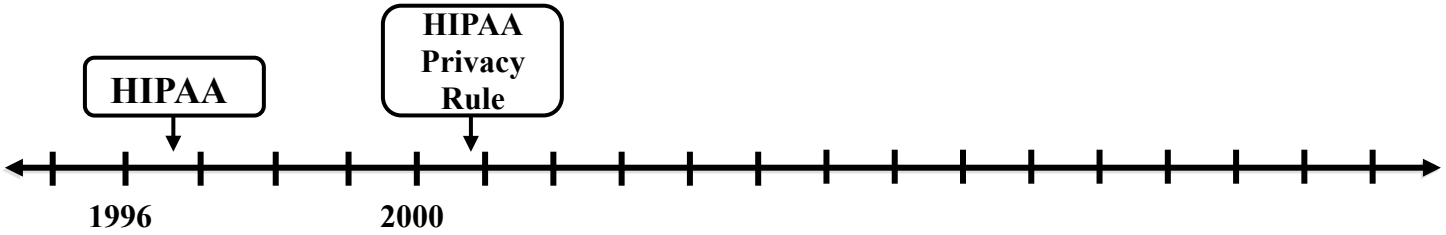
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996



- What are HIPAA "covered entities"?
  - Health plans.
  - Health care providers transmitting health information in electronic form in connection with a covered transaction.
  - Health care clearinghouse (i.e., companies that process/transmit health information).

HIPAA PRIVACY RULE

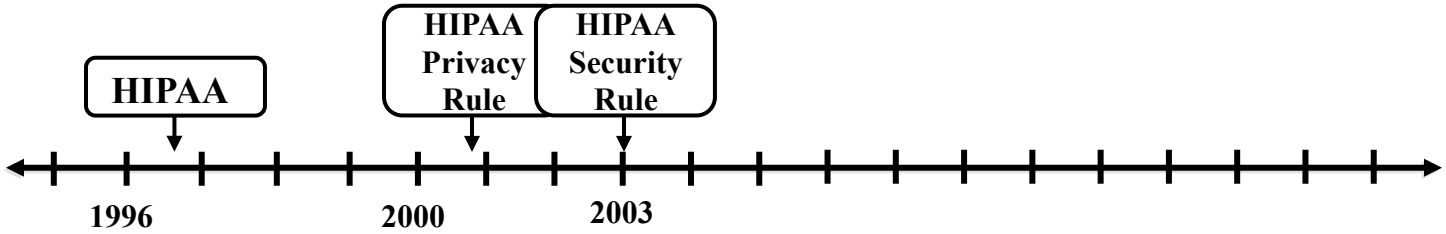
HIPAA PRIVACY RULE



- Privacy Rule
  - Prohibits unauthorized use of disclosure of PHI.

HIPAA SECURITY RULE

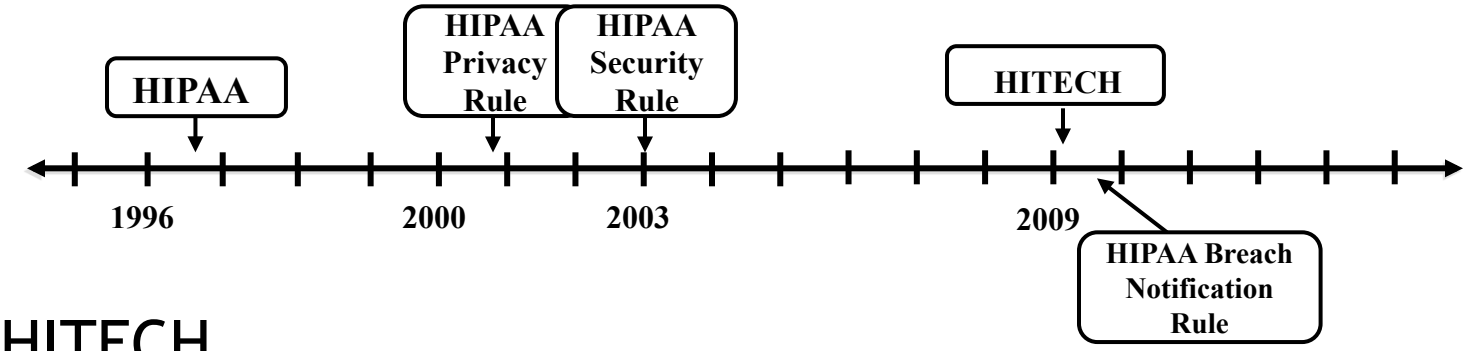
HIPAA SECURITY RULE



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

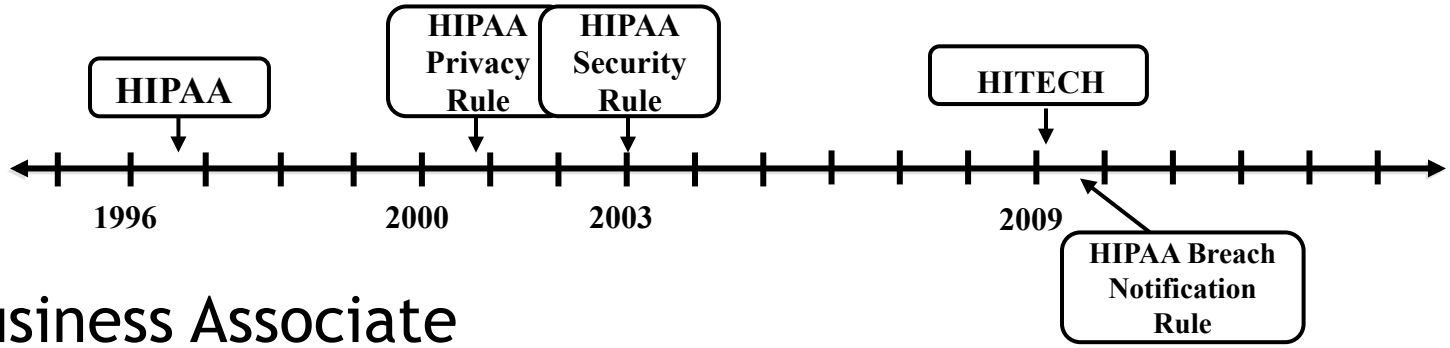
HITECH

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT



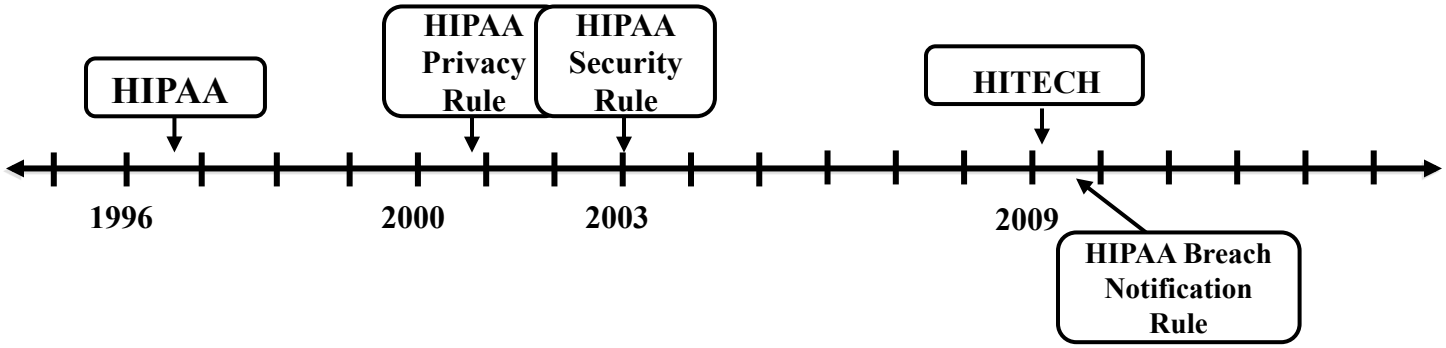
- HITECH
  - Passed by Congress in early 2009, as part of stimulus bill, to provide monetary penalties for HIPAA violations.
  - Extended HIPAA Privacy Rule and Security Rule to "business associates."
  - Called for implementation of HIPAA Breach Notification Rule, which was released by HHS in August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

HITECH 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."

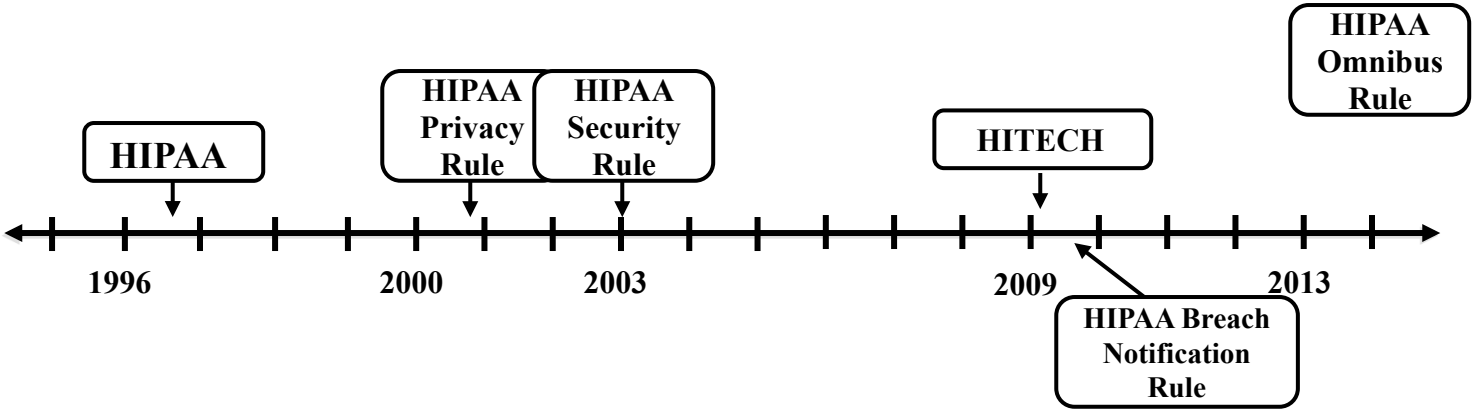
HITECH ACT



- Effect of HITECH on Business Associates
  - Privacy Rule
    - No unauthorized use or disclosure of PHI.
  - Security Rule
    - Must take affirmative steps to protect e-PHI.
  - Breach Notification Rule
    - Must provide appropriate notice of unauthorized acquisition, access, use or disclosure of PHI.

HIPAA OMNIBUS RULE

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

HIPAA RESTRICTIONS ON MARKETING

HIPAA RESTRICTIONS ON MARKETING

- HIPAA applies to any patient … no matter how old or how young … and whether the patient is covered by Medicare or commercial insurance. In other words, HIPAA is not limited to Medicare patients.

HIPAA RESTRICTIONS ON MARKETING

- HIPAA requires "covered entities" to obtain a valid authorization from individuals before using or disclosing protected health information ("PHI") to market a product or service to them.

HIPAA RESTRICTIONS ON MARKETING

- HIPAA defines “marketing” as:
  - “a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.” 45 CFR 164.501
  - The proposed rule referenced “health and non-health items and services”; the final rule deleted the reference.

HIPAA RESTRICTIONS ON MARKETING

- HIPAA broadly defines “use” of PHI to include the sharing, employment, application, utilization, examination, or analysis of such information. 42 CFR § 160.103.

HIPAA RESTRICTIONS ON MARKETING

- The new HIPAA definition of marketing states what is not marketing:
  - Marketing does not include a communication made:
    - For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication[,] …
      - Note: if there is financial remuneration related to the communication (e.g., a payment by a device manufacturer or advertising broker to a physician or supplier) then even treatment or operations related communications constitute "marketing" and will require a prior authorization.

HIPAA RESTRICTIONS ON MARKETING

- Marketing does not include a communication made (cont'd):
  - Communications by the provider specifically related to the circumstances of a particular individual for treatment purposes or furthering the individual's care.
    - This Includes activities such as referrals, prescriptions, recommendations, and other communications that address how a product or service may relate to the individual's health.
    - Example: A pharmacy or other health care provider mails prescription refill reminders to patients, or contracts with a mail house to do so.

HIPAA RESTRICTIONS ON MARKETING

- Marketing does not include a communication made (cont'd):
  - Communications made by a covered entity for the purpose of describing its network, the scope of products and services it provides, or the services for which it pays.
    - Example: A health plan sends a mailing to subscribers approaching Medicare eligible age with materials describing its Medicare supplemental plan and an application form.

HIPAA RESTRICTIONS ON MARKETING

- Marketing does not include a communication made (cont'd):
  - Communications made by the provider or health plan to an individual with regards to managing the treatment of that individual or for recommending alternative treatments, therapies, providers, or settings of care.
    - Permits covered entities to discuss products or services in the course of managing an individual's care or providing treatment.
    - Example: An endocrinologist shares a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the individual patient.

HIPAA RESTRICTIONS ON MARKETING

- Situational exceptions to "marketing" under HIPAA that do not require patient authorization:
  - HIPAA regulations describe two situations that fall within the definition of "marketing" but are excluded from the authorization requirement.
    - In other words, if a covered entity's "marketing" activities fit within one of the following situations, an authorization is not required.

HIPAA RESTRICTIONS ON MARKETING

- First Situation
  - Face-to-face communications with the individual, no authorization needed.
    - Example: Pharmacist tells patient about product or service when the patient is picking up a prescription at the pharmacy.
- Second Situation
  - Communications involving products or services of "nominal value" (Note: "nominal value" not defined in the rule), no authorization needed.
    - Example: Hospital provides a free package of formula and other baby products to new mothers as they leave the maternity ward.

HIPAA RESTRICTIONS ON MARKETING

- Therefore, to avoid HIPAA's requirement that the DME supplier obtain a valid authorization from the customer before making a marketing communication that does not involve face-to-face communication or a promotional gift of nominal value, the marketing communication must concern a health-related product or service (i) provided by the supplier and (ii) the supplier cannot receive financial remuneration in exchange for making the communication.

HIPAA RESTRICTIONS ON MARKETING

- If the "marketing" activity involves "financial remuneration" to the covered entity from a third party, the authorization must state that such remuneration is involved.
- "Financial remuneration" is defined as direct or indirect payment that flows from or on behalf of a third party whose product or service is being described, and does not include payment of the treatment of an individual.
  - Note: "financial remuneration" does not include non-financial benefits, such as in-kind benefits, only payments made in exchange for making such communication are included within the definition.

HIPAA RESTRICTIONS ON MARKETING

- When the Department of Health and Human Services revised the definition of marketing communication, it issued the following comments to the final rule:
  - We believe Congress intended that these provisions curtail a covered entity's ability to use the exceptions to the definition of "marketing" in the Privacy Rule to send communications to the individual that are motivated more by commercial gain or other commercial purpose rather than for the purpose of the individual's health care, despite the communication being about a health-related product or service.

HIPAA RESTRICTIONS ON MARKETING

- RECAP
  - The net result is that suppliers must generally obtain a valid prior authorization from the individual before using or disclosing the individual's PHI for "marketing" purposes, unless the "marketing" communication fits within an exception or is made is certain situations.
  - When "financial remuneration" is received by the supplier from a third party, the prior authorization must contain the standard required elements for a valid authorization under HIPAA and state that remuneration from a third party to the covered entity is involved in this use or disclosure.

HIPAA RESTRICTIONS ON SALE OF PHI

HIPAA: MARKETING VS. SALE OF PHI

- Important note:
  - HIPAA distinguishes between the use and disclosure of PHI for "marketing" purposes and the "sale of PHI."
    - As defined previously, "marketing" involves the use or disclosure of PHI to encourage the recipient to buy a product or service.
    - The "sale of PHI" is simply the disclosure of PHI in exchange for remuneration.
      - Note: "Remuneration" with regards to the "sale of PHI" includes both financial and non-financial, in-kind exchanges.

HIPAA RESTRICTIONS ON THE SALE OF PHI

- The HIPAA Privacy Rule requires a covered entity or business associate to "not use or disclose protected health information, except as permitted or required."
- It is not uncommon for a DME supplier to accumulate a large database of patients that it has sold products to in the past.
- This database of patients ("patient list") will likely include Medicare patients, Medicaid patients, and commercial insurance patients.

HIPAA RESTRICTIONS ON THE SALE OF PHI

- Assume that the DME supplier would like to monetize the portion of the patient list that does not include patients covered by a government health care program.
- Assume that the DME supplier desires to sell patient lists to laboratories that likely contain protected health information, such as patient names, telephone numbers, email addresses, medical conditions, health insurer information, or other information that may be used to market laboratory services.

HIPAA RESTRICTIONS ON THE SALE OF PHI

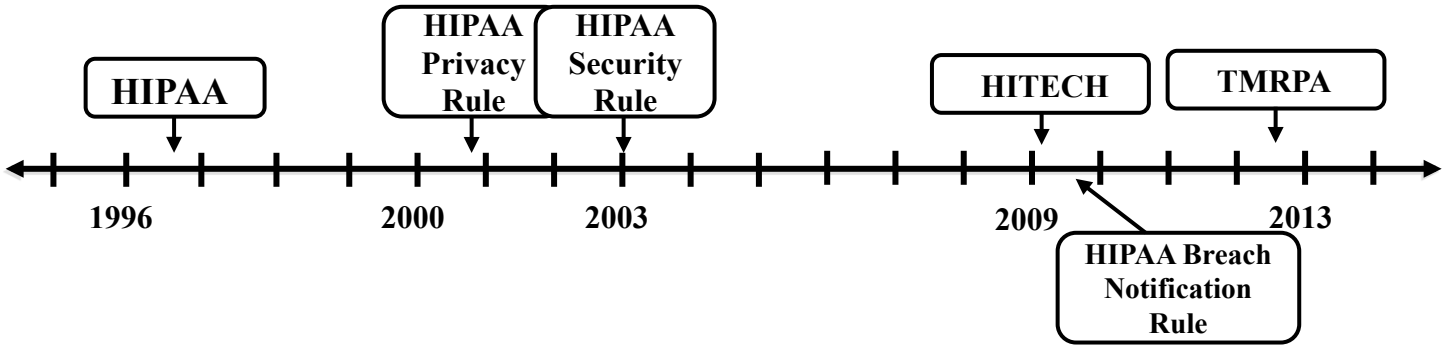
- Such information may only be disclosed if permitted by the HIPAA Privacy Rule.
- The HIPAA Privacy Rule permits the sale of PHI, with a valid authorization.
- A valid authorization for the sale of PHI must be written in plain language and include a laundry list of information, including at statement that such remuneration is involved.

STATE RESTRICTIONS ON MARKETING

STATE RESTRICTIONS ON MARKETING

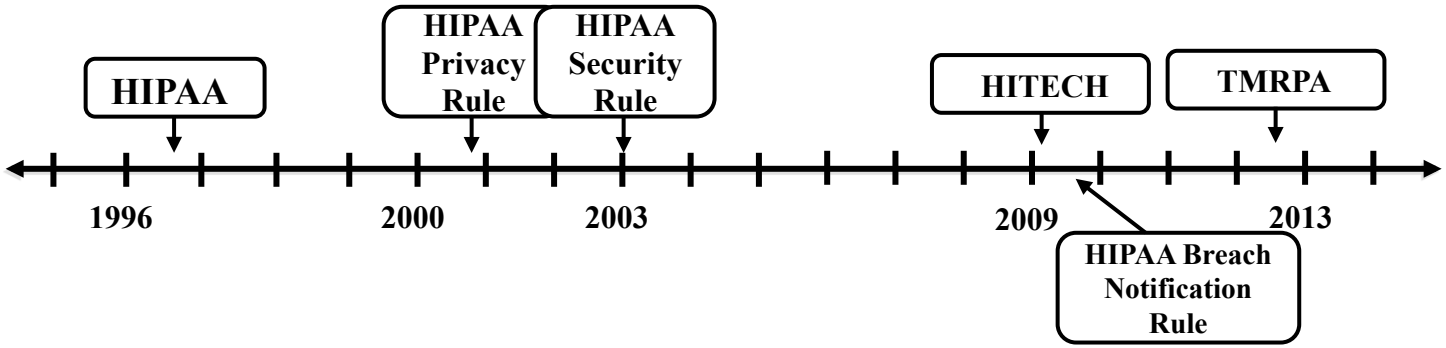
- In addition to the federal regulations created under HIPAA, states may issue additional laws and regulations designed to address patient information.
- While state law cannot conflict with federal law, states can add additional requirements or restrictions on the use of patient information and may expand regulations to address situations, information, patients, and entities not covered under federal laws and regulations.
- Even if the marketing activity in question is exempted from or not covered by HIPAA, be sure to check state law before using patient information.

STATE RESTRICTIONS ON MARKETING



- 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.
  - Broader in scope than HIPAA.

STATE RESTRICTIONS ON MARKETING



- Expanded definition of "Covered Entity"

Any person who

a) for commercial, financial, or professional gain … Engages, in whole or in part, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate … ;

STATE RESTRICTIONS ON MARKETING

b) comes into possession of protected health information;
c) obtains or stores protected health information under this chapter; or
d) is an employee, agent, or contractor of a person described [above] insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.

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

STATE RESTRICTIONS ON MARKETING

- Marketing
  - Marketing – similar, but not exactly as defined under HIPAA'
    - Includes
      - An arrangement between a covered entity and any other entity under which the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or services that encourages recipients of the communication to purchase or use that product or service; and

STATE RESTRICTIONS ON MARKETING

- Notwithstanding other exceptions that allow for communications for treatment, case management or care coordination, marketing includes "a product-specific written communication to a consumer that encourages a change in products."

Tex. Health & Safety Code § 181.001(b)(4)

STATE RESTRICTIONS ON MARKETING

- Enforcement and Penalties
  - Texas Attorney General may seek injunctive relief and assess civil penalties for violations. The penalties may not exceed:
    - $5,000 for each negligent violation that occurs within one year;
    - $25,000 for each knowing or intentional violation that occurs within one year; or
    - $250,000 for each knowing or intentional violation where PHI was used for financial gain.

FOREIGN RESTRICTIONS ON MARKETING

FOREIGN RESTRICTIONS ON MARKETING

- General Data Protection Regulation (GDRP)
  - Applies to all Member States of the European Union (EU)
  - Replaces the Directive 95/46/CE (Directive)
- As the title indicates, the GDRP is a “general” regulation that applies to the collecting and processing of personal data by all kinds of entities in all activities, including in the health care sector.

FOREIGN RESTRICTIONS ON MARKETING

- Extra Territorial Effect
  - The GDRP is much broader in scope than the Directive. The GDRP applies to companies that offer goods or services to individuals within the EU and/or monitor the behavior of data subjects within the EU, regardless of whether the companies were established within the EU
    - In other words, even a US company will be required to comply with the GDRP if it provides goods and services or targets European consumers.

FOREIGN RESTRICTIONS ON MARKETING

- Data Concerning Health
  - "means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."
  - "Member States may maintain or introduce further conditions, including limitations, with regard to processing of genetic data, biometric data or data concerning health."

FOREIGN RESTRICTIONS ON MARKETING

- Data Concerning Health
  - "Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."

FOREIGN RESTRICTIONS ON MARKETING

- Keys for marketing under the GDRP
  - Data Permission
  - Data Access
  - Data Focus

FOREIGN RESTRICTIONS ON MARKETING

- Keys for marketing under the GDRP
  - Data Permission
    - Customers must express consent in a "freely given, specific, informed, and unambiguous" manner, such as "by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website … . Silence, pre-ticked boxes or inactivity should not therefore constitute consent … . When the processing has multiple purposes, consent should be given for all of them."

FOREIGN RESTRICTIONS ON MARKETING

- Keys for marketing under the GDRP
  - Data Access
    - The "right to be forgotten"
      - "In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purpose for which they are collected or otherwise processed, where a date subject has withdrawn his or her consent or objects to the processing of personal data … ."
      - "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

FOREIGN RESTRICTIONS ON MARKETING

- Keys for marketing under the GDRP
  - Data Focus
    - "Any processing of personal data should be lawful and fair. . . . In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed … . In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

FOREIGN RESTRICTIONS ON MARKETING

- RECAP
  - Similar to HIPAA, the GDPR is applicable in all EU States and sets the minimum standards with regards to personal data.
  - The GDRP applies to all companies located within the EU and companies located outside the EU that provide products and service to individuals within the EU.
  - Individual EU states can implement additional regulations with regards to personal data, including data concerning health.

ACCREDITATION UNIVERSITY

QUESTIONS?

ACCREDITATION UNIVERSITY

THANK YOU

Denise M. Leard, Esq.
Brown & Fortunato, P.C.
905 S. Fillmore St., Ste. 400
Amarillo, Texas 79101
dleard@bf-law.com
806-345-6318

2CV1832