Morgan Lewis

HEALTHCARE PRIVACY RULES AND COORDINATING CARE

Tampa Bay Health and Medical Coalition
Reece Hirsch, CIPP, Co-head of Privacy & Cybersecurity Practice
May 9, 2019

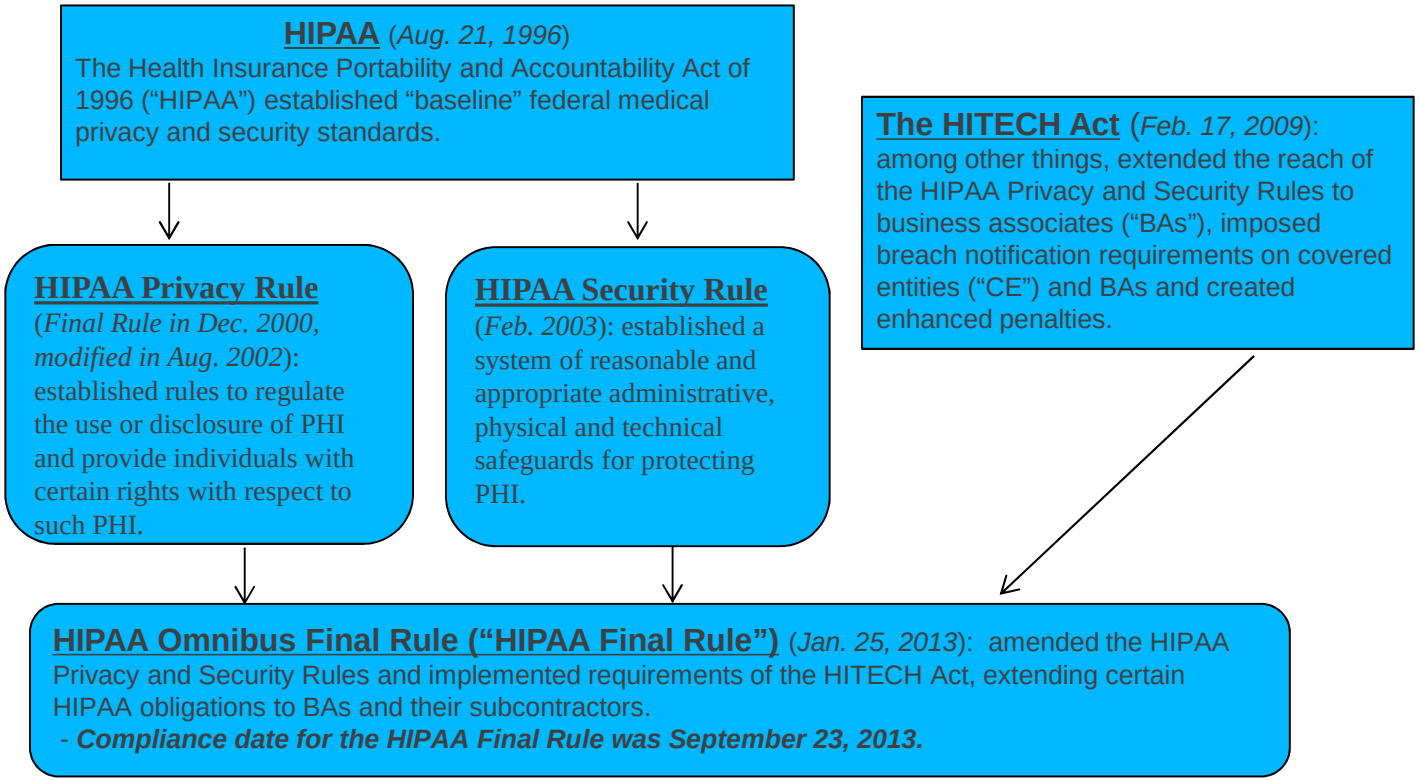
Objectives

- Overview of HIPAA
- Review HIPAA Rules governing disclosures for treatment, payment and health care operations
- Rules governing disclosure of substance use disorder (SUD) information
- Emergencies, declared disasters and mass shootings
- Public health disclosures
- How to prepare for emergencies from a privacy and security perspective

What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is the federal medical privacy law
- HIPAA was enacted to:
  - Increase efficiency and effectiveness of the health care system
  - Protect the privacy and provide for the security of PHI
  - Establish standards for accessing, storing and transmitting medical data and ensuring the security and privacy of PHI

The HIPAA Legal Timeline



What is the purpose of the HIPAA Privacy and Security Rules?

- **Individual Rights**:
  - To provide individuals with certain rights to their health information, including access to, and amendment of, such information.
- **Restrict Uses and Disclosures of PHI**
  - To restrict how covered entities and business associates can use or disclose such information
- **Security Safeguards**
  - To create a system of safeguards for securing such information

The HIPAA Privacy and Security Rules

- **Privacy**: refers to WHAT is protected – health information about an individual, restrictions placed on WHO may use, disclose or access the information

- **Security**: refers to HOW information is safeguarded – system of administrative, physical and technical safeguards for *electronic* protected health information

What Information is Protected by HIPAA?

- **Protected health information ("PHI")** is individually identifiable health information about an individual that is transmitted or maintained in ***any*** form (electronic, oral or written) where the information:
  - Is created or received by a health care provider, health plan, employer or health care clearinghouse;
  - Relates to:
    - An individual's **health or condition**
    - **Provision of health care** to an individual
    - **Payment for health care** to an individual; ***and***
  - Identifies an individual, or there is a reasonable basis to believe it can be used to identify an individual
  - But not de-identified information

PHI – individual identifiers

- What are the individual identifiers?
  - Names
  - Geographic subdivisions smaller than a state:
    - Street address
    - City
    - County
    - Precinct
    - Zip code, except for the initial 3 digits
  - Dates, except year
    - Birth date
    - Admission date
    - Discharge date
    - Date of death
  - Telephone numbers

PHI – individual identifiers (cont'd)

- What are the individual identifiers (cont'd)?
  - Fax numbers
  - E-mail addresses
  - SSNs – Social Security Numbers
  - Medical Record Numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - VIN and serial numbers, including license plate numbers
  - Device identifiers and serial numbers
  - Web universal resource locations
  - Internet protocol (IP) address numbers
  - Biometric identifiers, including finger and voice prints
  - Full face photographic images and any comparable images
  - Any other unique identifying number, characteristic or code

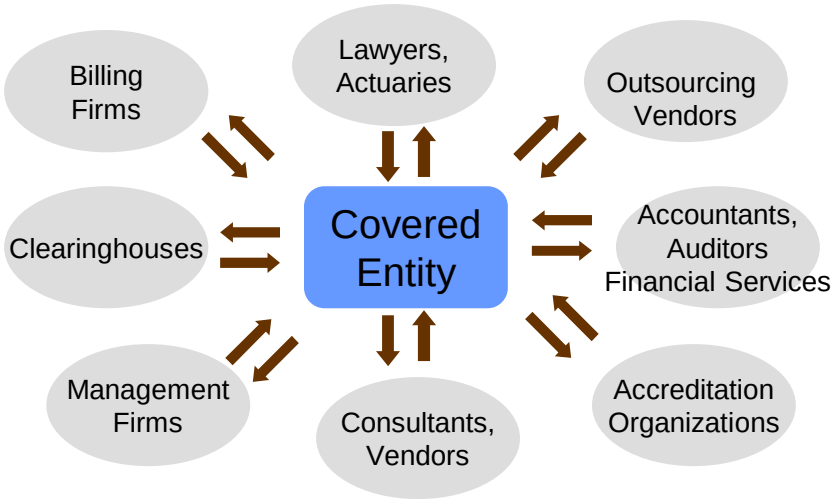
Who is Regulated by HIPAA?

What is a Covered Entity?

- Health plans (HMOs, employer group health plans)
- Health care providers that engage in standard electronic transactions (hospitals, medical groups)
- Health care clearinghouses

Who Is a Business Associate?

- A person or organization, *other than a member of a covered entity's workforce,* that ***creates***, ***receives***, ***maintains*** or ***transmits*** PHI on behalf of a covered entity for a function or activity regulated by HIPAA.
- A covered entity must have **business associate agreements** in place with all of its business associates, ensuring that the business associate will maintain confidentiality of all PHI.
- Under the Final Rule, a business associate also includes **subcontractors** of a business associate.
- A business associate may also be a covered entity



Minimum Necessary

- A covered entity shall request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the requested use or disclosure, in accordance with HIPAA's "minimum necessary" standard

Internal Requirements	External Requirements
Identify workforce who need access to PHI	Limit access to what is needed to accomplish the purpose for which the request was made
For each class/category of person identified, limit access based on need-to-know	Each request that is non-routine should be reviewed by the Privacy Officer

Uses and Disclosures

- The HIPAA Privacy Rule permits the use or disclosure without an authorization for the following purposes:
  - Treatment
  - Payment
  - Health Care Operations

These are often referred to as "TPO"

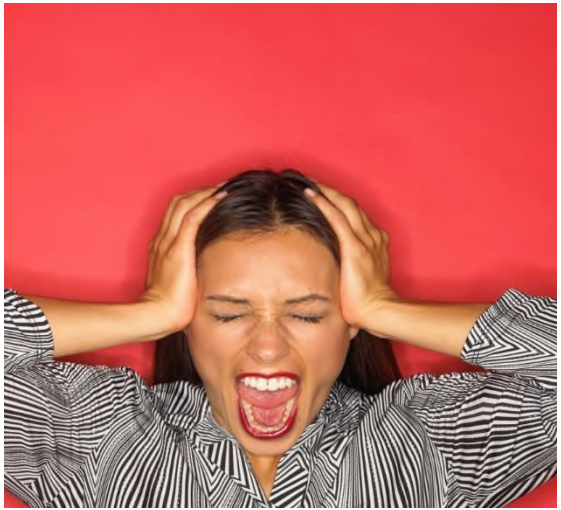
HIPAA Authorization Form

- An authorization is a written document, signed by the patient or his/her personal representative, giving permission to a covered entity to disclose PHI to a third party for a specific reason.
- A covered entity must obtain express authorization for disclosure of PHI that is not for TPO or not otherwise permitted by HIPAA.
- The authorization must be in writing, and the form must include certain elements required by HIPAA.
- A covered entity may not condition treatment upon authorization.
- The authorization is revocable at will at any time.

Security Rule Compliance

- Necessary steps for Security Rule compliance include:
  - Conducting a formal security **risk assessment**;
  - Implementing **written policies and procedures** with respect to Security Rule standards;
  - Providing **security training** to workforce members
  - Appointing a **Security Officer** to oversee Security Rule compliance efforts

The Dreaded Security Breach



The HIPAA Breach Notification Rule

- Covered entities are required to notify individuals whose "unsecured PHI" has been, or is reasonably likely to have been:
  - Accessed, acquired or disclosed as a result of a breach

- Unlike many state laws, applies to breaches involving both electronic and paper records.

What Is A Breach?

- "**Breach**" is defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information.

- **Notices** must be provided to the:
  - Affected individuals
  - Media, if the breach involves > 500 residents in a state
  - Secretary of Health and Human Services

Penalties

- **Civil**
  - $100 to $50,000 per violation per person up to a maximum of $1,500,000 per person per year per standard violation
  - Good news: on April 23, 2019, OCR issued a Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties that reduced the annual limit amounts for HIPAA civil penalties
    - For violations due to willful neglect that were corrected, the limit was reduced from $1.5 million per year to $250,000
- **Criminal**
  - Up to $50,000, 1 year in prison, or both, for inappropriate use of PHI
  - Up to $100,000, 5 years in prison, or both for using PHI under false pretenses
  - Up to $250,000, 10 years in prison or both, for the intent to sell or use PHI for commercial advantage, personal gain, or malicious harm

HIPAA TPO Disclosures

- A HIPAA covered entity may use or disclose PHI for its own
  - Treatment
  - Payment
  - Health care operations
    - Collectively referred to as "TPO"

Treatment Defined

- The provision, 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

Treatment Defined (cont.)

- Consultation between health care providers relation to a patient
- The referral of a patient for health care from one health care provider to another

Payment Defined

- Activities of a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits
- Activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of healthcare

Payment Defined (cont.)

- Determinations of eligibility or coverage (including COB)
- Adjudication or subrogation of health benefit claims
- Billing
- Claims management
- Collection activities

Payment Defined (cont.)

- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges

- Utilization review activities

Health Care Operations Defined

- Extensive definition with many components, including
  - Conducting quality assessment and improvement activities
  - Outcome evaluation and development of clinical guidelines
  - Population-based activities relating to improving health or reducing health care costs

Health Care Operations Defined (cont.)

- Protocol development
- Case management and care coordination
- Reviewing competence or qualifications of health care providers
- Medical review, legal services and auditing functions
  - Including fraud and abuse detection and compliance programs

Treatment of a Health Care Provider

- A covered entity may disclose PHI for treatment activities of a health care provider
  - Not necessarily a covered entity health care provider

Payment Activities of Receiving Entity

- A covered entity may disclose PHI to another covered entity or a health care provider for the payment activities of the entity that receives the information

Health Care Operations of Receiving Entity

- A covered entity may disclose PHI to another covered entity for health care operations activities of the entity receiving the information, IF
  - Each entity has or had a relationship with the individual who is the subject of the PHI
  - The PHI pertains to that relationship

Health Care Operations of Receiving Entity (cont.)

- And the disclosure is for a subset of health care operations that includes
  - Quality assessment and improvement
  - Case management and care coordination
  - Reviewing competence of health care professionals
- OR for the purpose of health care fraud and abuse detection or compliance

The History of Part 2

- In 1970 and 1972, Congress enacted
  - The Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act
  - The Drug Abuse Prevention and Rehabilitation Act of 1972
- Designed to protect the privacy of alcohol and drug abuse records
  - Ensure that persons with substance use disorders (SUD) are not dissuaded from seeking treatment due to fear of stigma
- 1975: US Dept. of Health, Education and Welfare issues the Confidentiality of Alcohol and Drug Abuse Records regulations, located at 42 CFR Part 2

Part 2 Regulations

- The Part 2 regulations set forth the limited circumstances in which SUD patient information may be used, disclosed and re-disclosed
- Until recently, regulations had not been substantively amended for nearly three decades
- Many providers argued that Part 2 had become outdated in the wake of the Health Insurance Portability and Accountability Act (HIPAA)

Updating the Part 2 Regulations

- January 18, 2017: US Dept. of Health and Human Services (HHS) Substance Abuse and Mental Health Services Administration (SAMSHA) released final regulations revising Part 2 (the Final Rule)
  - Intended to facilitate disclosure of SUD information between providers, patients and payors
  - More consistent with HIPAA but still recognizing sensitive nature of SUD information
  - Effective March 21, 2017
  - Further Part 2 amendments became effective February 2, 2018

Part 2 as a Barrier to Integration

- Prior to the recent regulations, Part 2 had become a barrier to integration of substance abuse treatment with health care decisions affecting the whole patient
- Part 2 was no longer consistent with the trend toward health information exchange
- Two disparate sets of privacy standards had served to isolate SUD treatment programs from other providers

What is a "Program"?

- A "program" is defined as any "individual" or "entity" that "holds itself out as providing education, treatment or prevention to individuals in need of alcohol or drug abuse treatment"
- A general medical facility is typically not considered a program
  - A defined unit within a general facility that holds itself out as a provider of substance abuse and/or alcohol treatment services and provides those services is a program under Part 2
- Specific providers working in a general medical facility whose main job function is to diagnose and treat patients for SUD meet the definition of "program"

"Federally Assisted"

- A program must be "federally assisted," which means that the program:
  - Is being operated by a department or agency of the US
  - Is operating based on the authorization of a department or agency of the US
    - *e.g.*, the program has received a license, certification, registration or other authorization from the government
  - Is receiving federal financial assistance or is part of an organization receiving federal financial assistance OR
  - Receives tax deductions or is operating under tax-exempt status

Examples of Federally Assisted Programs

- A program authorized, certified, licensed, or registered by the federal government
- A program receiving federal funds in any form, including funds that do not directly pay for SUD services
- Any program granted tax-exempt status by the IRS
- A program allowed tax deductions by the IRS for contributions
- A program authorized to conduct business by the federal government, including programs certified as a Medicare provider
- A program authorized to conduct methadone maintenance treatment
- A provider registered with the Drug Enforcement Agency
- A program conducted by the federal government

Interaction Between HIPAA & Part 2

- A provider that is subject to both HIPAA and Part 2 must follow both regulations
- The practical effect is that compliance with both regulations will necessarily mean adherence to the regulations with the most restrictions
  - Likely Part 2
- HIPAA's definition of "health information" is very broad, including any information that relates to
  - The past, present or future physical or mental health condition of an individual
  - The provision of health care to an individual
  - The past, present or future payment for the provision of health care to an individual

Information Subject to Part 2

- Information protected by Part 2 overlaps with HIPAA but is narrower in scope
- Information that identifies individuals who have received treatment or are receiving treatment for substance abuse and/or alcohol abuse
- "[Records] of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of [drug abuse and/or alcohol abuse] programs"

Medical Emergencies

- Prior to the Final Rule, Part 2 provided that SUD information may be disclosed to medical personnel
  - "For the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention"
- Final Rule modifies the medical emergencies provision to reflect the statutory language that Part 2 information may be disclosed to medical personnel without patient consent to the extent necessary to meet a "bona fide medical emergency"
  - Intended to give providers greater discretion to determine when a medical emergency exists

Balancing Part 2 and HIPAA

- SAMHSA is still trying to strike the right balance between Part 2 protections for SUD information and more permissive HIPAA rules that are more consistent with treatment obligations
- Particularly in the context of the opioid crisis, expect further changes to Part 2 requirements
- In its guidance regarding HIPAA disclosures in disasters, OCR notes that Part 2 may still impose more stringent requirements

HIPAA and Disaster Response

- OCR has issued several guidance documents in response to a series of natural disasters and high-profile emergency situations
  - Hurricanes Harvey, Irma and Maria, California wildfires
  - In response to these natural disasters, the following HIPAA requirements were waived on a temporary basis during the public health emergency
    - Distributing the Notice of Privacy Practices
    - Honoring a request to opt out of a facility directory
    - Obtaining the patient's agreement to disclose information to family members or friends involved in patient's care
    - Patient's right to request privacy restrictions and confidential communications

When Can A HIPAA Waiver Be Declared?

- The President must declare an emergency or disaster AND
- The Secretary of HHS must declare a public health emergency
- Issuance of a waiver means that HIPAA sanctions and penalties will not be imposed on a covered entity hospital that does not comply with the waived privacy provisions

Scope of a HIPAA Waiver

- If the Secretary of HHS issues a HIPAA waiver with respect to a disaster or emergency, it only applies:
  - In the emergency area and for the emergency period identified in the public health emergency declaration\
  - To hospitals that have instituted a disaster protocol
    - The waiver applies to all patients at such hospitals

Scope of a HIPAA Waiver (cont.)

- Waiver extends for up to 72 hours from the time the hospital implements its disaster protocol
- When the Presidential or Secretarial declaration terminates, a hospital must then comply with all Privacy Rule requirements
  - Even if 72 hours has not elapsed since disaster protocol was implemented

Public Health Disclosures

- Even in the absence of a HIPAA waiver, covered entities may disclose PHI for treatment, payment and health care operations (TPO) purposes
- HIPAA also recognizes the need for certain public health-related disclosures of PHI

Disclosures to Public Health Authorities

- A covered entity may disclose PHI without an individual's authorization to a ***public health authority***, defined as:
  - An agency or authority of the US government, a state, a territory, or a political subdivision of a state, territory or Indian tribe, that is responsible for public health matters as part of its official mandate
  - Would include the CDC and state or local health departments

Types of Public Health Disclosures

- Public health disclosures could include
  - Reporting of disease or injury
  - Reporting vital events, such as births or deaths
  - Conducting public health surveillance, investigations or interventions
    - 45 C.F.R. § 164.512(b)(1)(i)

Disclosures to Persons at Risk

- A covered entity may disclose PHI without an authorization to
- Persons at risk of contracting or spreading a disease or condition
- If other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control disease or carry out public health interventions or investigations
- 45 C.F.R. § 164.512(b)(1)(iv)

Disclosures to Family, Friends and Others Involved in Care

- A covered entity may share PHI with a patient's family members, relatives, friends or other persons identified by the patient as involved in the patient's care
- A covered entity may also disclose PHI about a patient as necessary to identify, locate and notify family members, guardians or anyone else responsible for the patient's care
  - Such as information regarding the patient's location, general condition or death
  - Where necessary to identify family members and others, this may include disclosures to the police, press or public at large
  - 45 C.F.R. § 164.510(b)

Disclosures to Family, Friends and Others Involved in Care (cont.)

- The covered entity should get verbal permission from the individual or otherwise be able to infer that the patient does not object, when possible
  - if the individual is incapacitated or not available, the covered entity may share information for these purposes if, in its professional judgment, doing so is in the patient's best interest

Disclosures to Family, Friends and Others Involved in Care (cont.)

- For patients who are unconscious or incapacitated
  - A health car provider may share relevant information about the patient with family, friends or others involved in the patient's care or payment for care
  - If the provider determines, based on professional judgment, that doing so is in the best interests of the patient
  - Example: A provider may determine that it is in the best interest of an elderly patient to notify the patient's adult child of a hospitalization, but should not share unrelated medical information about the patient without permission

Disclosures for Disaster Relief

- A covered entity may share PHI with disaster relief organizations, like the American Red Cross, that are authorized by law or their charters to assist in disaster relief efforts
  - For the purpose of coordinating the notification of family members or other persons involved in the patient's care, of the patient's location, general condition or death
  - It is unnecessary to obtain the patient's permission to share the PHI if doing so would interfere with the organization's ability to respond to the emergency
  - 45 C.F.R. § 164.510(b)(4)

Disaster Relief Organizations and the Scope of HIPAA

- Remember that HIPAA only applies to health care providers, health plans and health care clearinghouses
- Once PHI has been appropriately disclosed to third parties like disaster relief organizations and law enforcement agencies, HIPAA restrictions no longer apply

Disclosures to the Media

- A covered entity health care provider may use the following PHI to maintain a facility directory of patients
  - Name
  - Location in the facility
  - Condition described in general terms (*e.g.*, critical or stable, deceased, or treated and released)
- HIPAA does not provide an exception that would permit further disclosures of PHI to the media without the patient's written authorization
- 45 C.F.R. § 164.510(a)

HIPAA and Mass Shootings

- January 2017: OCR issues updated guidance on permissible disclosures during emergency situations after December 2016 shootings at the Pulse nightclub in Orlando
  - Providers are permitted to disclose PHI to family members, friends, and other loved ones who are not married to the patient or otherwise recognized as relatives
  - Providers are not allowed to discriminate on the basis of sex or gender identity
- OCR reiterated and expanded on the hurricane disaster response guidance in October 2017 after the mass shooting in Las Vegas
  - OCR emphasizes that a formal HIPAA waiver is rarely required for an emergency situation like a mass shooting

Disclosures to Law Enforcement

- HIPAA contains exceptions for disclosures to law enforcement that would be applicable in mass shooting situations
  - As required by law (such as reporting of shootings and stabbings)
  - In response to a court order or subpoena

Disclosures to Law Enforcement (cont.)

- In compliance with the requirements of an authorized investigative demand or similar process, provided that
  - The information is relevant and material to a legitimate law enforcement inquiry
  - The request is specific and limited in scope to the extent reasonably practicable
  - De-identified information could not reasonably be used

Disclosures for Identification and Location Purposes

- A covered entity may disclose PHI in response to a law enforcement request to identify or locate a suspect, fugitive, material witness or missing person, provided that disclosure is limited to certain information, including
  - Name and address
  - Social Security number
  - Blood type
  - Type of injury
  - Physical characteristics, etc.

Preparing for Your Next Emergency

- Table-top exercises are often conducted to prepare for security breach scenarios, but they can also be valuable for emergency response situations
  - Particularly in states like Florida where emergencies like hurricanes are likely
- Consider incorporating privacy resources into your emergency response preparedness team
  - Meet in peacetime and work through these HIPAA and Part 2 issues when you aren't under the pressure of a crisis!
- HIPAA does not have to serve as a barrier to coordination of care in an emergency, but you have to develop a familiarity with the rules

Contact Info

Reece Hirsch, Morgan, Lewis & Bockius LLP

San Francisco

T:1.415.442.1422

F:1.415.442.1001

THANK YOU