Privacy Obligations and Restrictions For In-House Legal Advisors Under the Texas Medical Records Privacy Act and HIPAA

October 24, 2019

Prepared by:

Jeffery P. Drummond
Jackson Walker L.L.P.
2323 Ross Ave., Suite 600
Dallas, Texas 75201
(214) 953-5781
jdrummond@jw.com
www.hipaablog.blogspot.com

HIPAA Background and History

A brief history of HIPAA

- 1996: HIPAA statute passes
- 2000/2001: Privacy Rule published
- 2003: Privacy Rule enforceable, Security Rule published
- 2005: Security Rule enforceable
- 2009: HITECH Act passes, initial regulations passed
- 2013: HITECH “omnibus rule” published

Statutes from Congress Regulations from HHS

The Privacy Rule

Privacy Regulations in General Cover:

- Rules for the disclosure and use of PHI
- Individual rights regarding protected health information
- Administrative Safeguards (responsibilities of CEs and BAs)

JACKSON WALKER L.L.P.

The Privacy Rule: The "Rule"

- An absolute prohibition with exceptions:
- "Thou shalt not": A covered entity may not use or disclose PHI, except –
  - For treatment, payment, or healthcare operations
  - With the individual's authorization or to the individual
  - As otherwise required by law or otherwise permitted or required under the privacy regulations

The Privacy Rule: the "Rights"

- Individuals have the right to receive a Notice of Privacy Practices
  - Describes individual's rights to access, inspection, accounting
  - Describes duties of covered entity
  - Instructs how to file complaints and make contact
  - Describes how covered entity will use and disclose the patient's health information
- Information cannot be used or disclosed for any purpose not included on the Notice.
- Individual must be notified if information is used in a new fashion not covered by the old Notice

JACKSON WALKER L.L.P.

Privacy Standards: Individual Rights

Right to Access own Information

Right to Request Amendment

- Accepting amendments
- Denying amendments
- Grounds for denial

Right to Request Restrictions

- Can refuse, but see the "Hide Rule"
- If agree, are bound to it

Right to Request Communications in alternative fashion

- Correspondence sent to alternate address
- Must accommodate reasonable requests

Right to Receive an Accounting of Disclosures

- Date and purpose
- Recipient name
- Description of information disclosed
- Exceptions for treatment, payment and health care operations
- Exception for disclosures pursuant to an Authorization

The Privacy Rule: the "Responsibilities" of Covered Entities

- Enter Business Associate Agreements
- Appropriate documentation (NoPP, authorizations)
- Adopt Policies and Procedures
- Training of Employees
- Privacy Officer and Security Officer
- Document complaints
- Comply with the Security Rule

The Privacy Rule: Odds and ends

- "Minimum Necessary" rule: except for disclosures for treatment, Covered Entities must limit all permitted disclosures to the "minimum necessary" to accomplish the purposes of the disclosure.
- Patient authorizations (for disclosures other than treatment, payment, healthcare operations, or required by law) must contain specific elements.
- Almost all disclosures for marketing purposes require a specific authorization.

The Security Rule

JACKSON WALKER L.L.P.

The Security Rule

- Covered entities must establish policies and procedures and put in place safeguards to secure the PHI they maintain and transmit.
- A "risk analysis" is the first step in the process to determine what risks exist and how they can be mitigated.
- Then, safeguards must be put in place.

JACKSON WALKER L.L.P.

Addressable vs Required

- CEs and BAs must adopt administrative, physical, and technical safeguards to reasonably protect the confidentiality, integrity and availability of PHI
- Regulations are “technologically neutral”
- Regulations are divided into “required” and “addressable” categories (the ones underlined below are required, the rest are addressable).

Administrative Safeguards

- Security Management Process
  - Risk Analysis
  - Risk Management
  - Sanction Policy
  - Information System Activity Review
- Assigned Security Responsibility
- Workforce Security
  - Authorization and Supervision
  - Workforce Clearance Procedure
  - Termination Procedure
- Information Access Management
  - Isolating Clearinghouse Function
  - Access Authorization
  - Access Establishment and Modification

Administrative Safeguards (cont.)

- Security Awareness and Training
  - Security Reminders
  - Protection from Malicious Software
  - Log-in Monitoring
  - Password Management
- Security Incident Procedures
  - Response and Reporting
- Contingency Plan
  - Data Backup Plan
  - Disaster Recovery Plan
  - Testing and Revision Procedure
  - Applications and Criticality Analysis
- Evaluation
- Business Associate Contracts

Physical Safeguards

- Facility Access Controls
  - Contingency Operations
  - Facility Security Plan
  - Access Control and Validation Procedures
  - Maintenance Records
- Workstation Use
- Workstation Security
- Device and Media Controls
  - Disposal
  - Media Re-use
  - Accountability
  - Data Backup and Storage

Technical Safeguards

- Access control
  - Unique User Identification
  - Emergency Access Procedure
  - Automatic Logoff
  - Encryption and Decryption
- Audit controls
- Integrity
  - Mechanism to Authenticate E-PHI
- Person or Entity Authentication
- Transmission Security (encryption)

The Breach Notification Rule

- HITECH provisions of "Stimulus" Bill require notification in cases of breach (improper disclosure or access) of PHI
  - To the affected patient
  - To the media if the breach is big (over 500 people)
  - To HHS
- Breach of "secured" (encrypted) data need not be reported
- Breach of de-identified data need not be reported

Texas Medical Privacy Laws:

- **HIPAA** is the Health Insurance Portability and Accountability Act of 1996

- **TMRPA** is the Texas Medical Records Privacy Act

- **TITEPA** is the Texas Identity Theft Enforcement and Protection Act

All are relevant to in-house benefit and legal departments

What **is Protected by Medical Privacy Regulations?**

- HIPAA's privacy regulations protect "Protected Health Information" or "PHI" which is:
  - Individually identifiable health information ("IIHI");
  - Created or received by a HIPAA covered entity; and
  - Maintained in any form or medium
  - NOTE: HIPAA protects PHI for 50 years after the individual's death
- TMRPA uses this same definition.
- TITEPA deals with "Sensitive Personal Information," which includes a name and identifying number, and by definition includes PHI.

Who **is Covered by Medical Privacy Regulations?**

HIPAA (limited):

- –Direct applicability to "Covered Entities" (CEs)
  - •Physicians, hospitals and other healthcare providers that conduct electronic transactions
  - •Health insurance plans
  - •"Healthcare clearinghouses"
- –Direct (Security Rule) and indirect (Privacy Rule) applicability to "business associates"
- –Generally no applicability to employers

TMRPA (much broader):

- –Entity who, for commercial purposes, assembles, collects, or transmits PHI; or who possesses, obtains, or stores PHI
- –Excludes health plans, educational records, other entities

TITEPA (even broader):

- –Any business in Texas

TITEPA's Primary Requirements

- **Prohibits Identity Theft**

- **Requires businesses to reasonably protect sensitive personal information from unlawful use or disclosure**
  - –Safe destruction of SPI required

- **Requires breach notification**
  - –Computerized data breaches only

- **Provides some protections for victims of Identity Theft**

Medical Privacy Applies to:

- **HIPAA only**
  - –Group Health Plans

- **TMRPA only**
  - –Non-HIPAA covered entities other than:
    - •Excepted entities: group health plans, certain nonprofits, workers comp programs, Red Cross,
    - •Partially excepted entities: employers, certain insurers, financial institutions, employers

- **Both HIPAA and TMRP**
  - –Healthcare providers
  - –Healthcare clearinghouses

  (note, one entity may have components in each category)

Basic Rules of Medical Privacy:

DO NOT DISCLOSE OR USE (in a manner not permitted by the law) PROTECTED HEALTH INFORMATION- Not all Health Information is protected

KEEP MEDICAL INFORMATION SECURE

- **Ensure that persons outside of the groups who deal with a medical provider component of an entity or a health plans do not have the opportunity to see it.**
- **Persons providing services to the health plan and obtaining access to PHI must sign a business associate agreement (yes, law firms can be BAs).**

Application of Medical Privacy Laws Depends on Source of Information and Purpose of Receipt of Information:

- Employer
  - FMLA, IOD, Workers Compensation, Disability Management, Fitness for Duty, Random Drug Testing, Interventions for employee problems
  - ADA
- Medical records from treating employees as a health care provider- clinical records- vaccines, prescriptions, treatment
- One of the medical components of a Group Health Plans for active employees or retirees

Application of Medical Privacy Laws Depends on Source of Information and Purpose of Receipt of Information:

- Medical Records from a group health plan is protected health information from a "covered entity" under HIPAA and is subject to the HIPAA privacy and security rules which require disclosures to be limited to certain permitted or authorized disclosures and records to be kept of such disclosures or uses by the health plan.
- Medical records from the healthcare provider component of an employer require analysis of the source of the information and the purpose for which it was received to determine which laws and restrictions apply (depends on the functions of the healthcare provider component).

Examples:

- Fitness for Duty exam records- the healthcare provider component may be acting as the employer and the records of these exams may be disclosed to legal for use in disclosure to appropriate regulatory bodies (e.g., DOT for trucking, FAA for aviation) as a disclosure required by law – not restricted by HIPAA or TMRPA.
- Medical records the healthcare provider component receives from employees requesting an FMLA leave are received in its capacity acting as the employer and can be retained in the employee's medical files and used by the employer (including legal) -- not subject to HIPAA or TMRPA.

Examples:

- The healthcare provider component's clinical services, flu shots, prescriptions are services when acting as a health care provider and are subject to the TMRPA because they are received when the healthcare component provider is acting as a health care provider (but not subject to HIPAA as long as the healthcare component does not bill using the standard electronic transaction under HIPAA) – if these records are needed it is best to have the employee sign a HIPAA-compliant authorization form.
- Records of medical services provided to employees or dependents and paid for by the health plan are subject to HIPAA.

Examples:

- The employer may not use any PHI from the health plan for any other benefit or employment decision.
- An employee has the right to access his/her PHI that the plan possesses under HIPAA excepting any PHI gathered in anticipation of litigation or for use in civil, criminal or an administrative action or proceeding (45 CFR 164.524(a)). Such information gathered in anticipation of litigation, etc. is not required to be included when an individual requests access to their PHI held by the health plan.

Examples:

- An employee may authorize the health plan to provide his/her PHI to a third party if he/she signs an authorization (e.g., opposing counsel), however PHI compiled in anticipation of litigation is not required to by produced (note, this caveat is subject to any different obligation that may exist under a applicable collective bargaining agreement).

Examples:

- A health plan may disclose its PHI without the individual's agreement pursuant to a judicial or administrative process under 45 CFR 164.512(e) in response to an order of a court or administrative tribunal, provided the specific requirements are met, or if a court order is not included with a discovery request, subpoena, or other lawful process, if the health plan receives "satisfactory assurances" from the requesting party that reasonable efforts were made to notify the individual or a "qualified protective order" is obtained.
- If you need access to an employee's medical records from an outside health care provider or another plan and the employee will not sign an authorization, the mechanism to obtain such records is the one described above.

Privacy & Retention of Outside Counsel

- Health plans must keep protected health information private and secure both electronically and physically.
- If you retain outside counsel to represent a health plan in litigation, during a claim appeal process, a governmental inquiry or audit or related to vendor disputes where health plan data will need to be accessed, that outside counsel is a business associate to the health plan and must sign a business associate agreement before any PHI is provided to the outside counsel.

Privacy & Retention of Outside Counsel

- If outside counsel is retained for employment litigation and there is no claim against the health plan in the litigation, but access to health plan data is necessary (e.g., employee injured off duty and claims FMLA violation), have the employee sign an authorization to release the data -- no BAA (client is the employer, not the plan).
- If outside counsel is retained for a dispute regarding an employee's disability, the records in the employer's files relating to fitness for duty are obtained in its capacity as acting for the employer and are not subject to HIPAA -- no BAA.

Privacy & Retention of Outside Counsel

- If the retention is for a workers compensation claim, workers compensation is outside of HIPAA privacy- no BAA is required.
- If the retention is for defense of an ERISA 510 retaliation claim that may involve benefit health benefits- get a BAA.
- If the retention is for an arbitration related to a medical plan benefit claim- get a BAA.

Privacy Impacts Your Representation of Your Client

- If you are an attorney representing a client in litigation or in a grievance with an employee, you must know the source of the medical records you need to determine which rules apply and what you may need to do to obtain access such records.
- If you need to obtain medical records from an outside health plan or health care provider, you must comply with the requirements for obtaining the records via a judicial or administrative process or get the employee to sign an authorization permitting disclosure to you.

Privacy Impacts Operations of a Healthcare Provider component

- TMRPA restricts an employer's ability to access or use health data held by a healthcare provider component of the employer.
- TMRPA requires some separation between a company's activities taken as an employer and as a medical provider through a healthcare provider component.
- An employer may still use such medical information:
  - As required by law to comply with legal requirements (e.g., DOT or FAA fitness for duty)
  - To comply with OSHA or EPA requirements
  - For workers' compensation claims
  - As an employer to defend itself in litigation

Employment Records are Not PHI

- Records the company receives in its capacity as an employer are not Protected Health Information subject to HIPAA or TMRPA privacy regulations.
  - Examples: FMLA leave requests and medical certifications, requests for reasonable accommodations under the ADA, workplace safety surveillance and drug screening results.
- Employment medical records still must be kept private to comply with other laws (e.g., TITEPA).
  - Data collected by an employer's healthcare provider component must be limited to use for treatment or for recording or reporting an OSHA incident, workers' compensation claim, or similar workplace injury or accident.

Privacy Requires Training and Re-training

- Employees who have access to PHI must be trained to not use or disclose it other than as permitted
  - TMRPA requires employee training within 60 days of hire and whenever the employer's privacy requirements change
  - HIPAA requires training of new hires and periodic training thereafter
- HIPAA's 6 year record retention rule applies to records of its compliance with HIPAA

Individual Authorization Required to Disclose an Individual's PHI

- **Uses or Disclosures Requiring an Authorization**
  - General Rule**:** An authorization is required for any use or disclosure not for treatment, payment, healthcare operations, or otherwise permitted. The scope of the use or disclosure is governed by the terms of the authorization.
  - Healthcare provider component personnel must obtain an authorization from an individual (whose medical information it received as a health care provider) before it can be disclosed, if it is not a disclosure which is permitted under HIPAA or the TMRPA.

Medical Privacy Compliance

- Why should you care?
  - HIPAA:
    - Federal civil and criminal penalties
    - Private causes of action
    - Penalties may apply to individual employees
  - TMRPA:
    - State civil penalties

- State penalties are in addition to federal penalties when both are applicable

- Claims for violation of privacy rights under the common law have been permitted to proceed as not preempted by HIPAA by the U.S. Supreme Court

HIPAA Penalties: Why you Must Care

- Private Causes Actions
  - Some state laws permit individuals to sue for violations of their medical information privacy
  - State common law claims also are permitted

- Post 2-17-09, State Attorneys General may enforce HIPAA Privacy and HITECH, in addition to Federal Enforcement and may enforce state laws in addition to federal laws

Questions?

Thank you for your attention.

Privacy Obligations and Restrictions For In-House Legal Advisors Under the Texas Medical Records Privacy Act and HIPAA

October 24, 2019

Prepared by:

Jeffery P. Drummond
Jackson Walker L.L.P.
2323 Ross Ave., Suite 600
Dallas, Texas 75201
(214) 953-5781
jdrummond@jw.com
www.hipaablog.blogspot.com