Protected Health Information During a Pandemic: Is it Still Protected by HIPAA?

March 2020
Revised December 2020

Megan Neel, JD
Dumas Neel, PLLC
mneel@dumasneel.com
2950 N. Loop W. #500
Houston, TX 77092
(713) 462-0993
www.dumasneel.com

Author's note: This document was originally written to provide basic information about the Health Insurance Portability and Accountability Act (HIPAA)[1] and was intended for the general public, although it contains regulations and information that may be considered legal jargon to the layperson. Nothing in this document is to be construed as legal advice directed at any individual or covered entity. If the reader needs legal advice, they should contact an attorney.

Foreword: In December 2019, a virus known as COVID-19, or "Coronavirus" was detected in Wuhan, China. COVID-19 is a potentially fatal virus which has up to a two-week incubation period, and is fairly contagious, spreading through communities easily.[2] Beginning in late February 2020, individuals in the continental United States started testing positive for COVID-19. Since December 2019, COVID-19 has been detected in 218 countries, and has infected over 67 million people worldwide. The World Health Organization (WHO) declared COVID-19 a global pandemic on March 11, 2020. The same week, many major cities in the United States began "lockdown" measures, restricting what types of businesses could continue to operate.

Many healthcare providers, legal scholars, and individuals were concerned not only about how this virus would spread throughout their communities, but how to address some of the broader concerns of the public and their clients. This paper will broadly explain the responsibilities of healthcare providers and the local, state, and federal government during a pandemic. This paper will also discuss some of the Texas privacy laws and the obligations of covered entities, businesses, and public health authorities.

[1] Codified as 45 C.F.R. Parts 160 and 164

[2] https://www.cdc.gov/coronavirus/2019-ncov/about/transmission.html, accessed March 12, 2020

I. Background of HIPAA

In the fall of 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed, drastically changing the face of healthcare and many other healthcare-related businesses. When HIPAA was initially passed, there was a lot of confusion for many covered entities as to how they could protect the privacy of information in a way that was electronic. Internet Explorer was only a year old, Google was still a year away from being founded, and only 22% of individuals in the United States used the internet at work or at home – up from 15% the year before.[3] Despite the low numbers of individuals who were tech savvy in the United States, covered entities – defined as health plans, healthcare providers and healthcare clearinghouses - "that electronically transmit health information … to carry out financial or administrative activities related to health care" were required to follow the HIPAA regulations regarding data privacy.[4,5]

The first compliance dates for filing electronic claims with CMS began in 2003, which meant that covered entities filing Medicare claims had two years to become compliant with HIPAA and the Privacy Rule. Unsurprisingly, many covered entities were non-compliant, or did not implement appropriate safeguards, which required additional HHS rules and legislation over the next ten years, including the Enforcement Rule, passage of the Security Rule (known as "HITECH" to most), the Breach Notification Rule, the Omnibus Rule of 2013, and various penalties for non-compliance, including civil and criminal penalties.[6] In addition to the federal legislation and rules promulgated by HHS, many states passed laws that were more restrictive than HIPAA, including Texas. In 2011, the Texas Legislature passed HB

[3] https://www.people-press.org/1996/12/16/online-use/ Accessed June 6, 2020
[4] https://hipaa.bsd.uchicago.edu/background.html#:~:text=HIPAA%20was%20enacted%20as%20a,their%20health%20insurance%20between%20jobs. Accessed June 6, 2020
[5] 45 CFR 160.102-103
[6] Civil money penalties are set out in 45 CFR § 160.404; criminal penalties are set out in 42 USC § 1320d–6

300, later codified in Texas Health & Safety Code Chapter 181, known as the Texas Medical Records Privacy Act.

II. Texas Privacy Laws

Texas has some of the most restrictive laws in the United States when it comes to the protection of sensitive information, including health information. The Texas Medical Records Privacy Act ("TMRPA") has often been dubbed "Texas HIPAA" and greatly expanded the definition of a covered entity to include

any person who:

(A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site;

(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 by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.[7]

Interestingly, this definition includes schools, which already have existing obligations to protect records under the Family Educational Rights and Privacy Act

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

("FERPA"), and it also includes many businesses that would otherwise not be obligated to comply with privacy protections, such as attorneys.

The TMRPA requires that all Texas covered entities train employees and contractors (a) once every two (2) years and (b) within ninety (90) days of hire. This training is to be customized to the covered entity and is to cover state and federal law related to PHI. The TMRPA also requires that the time frame in which a covered entity has to respond to a request for disclosure of PHI is fifteen (15) days, which is less than the thirty (30) days required by HIPAA.[8] Finally, covered entities as defined by the chapter, including individuals, are subject to investigation and disciplinary proceedings, including revocation of a license or civil penalties for failure to adhere to privacy standards.[9] For the purposes of this paper, the term "covered entity" includes both the definitions in HIPAA and Texas law.

HIPAA protects certain information, known as "protected health information," or "PHI" and prevents covered entities from disclosing this information to others. There are some exceptions where a covered entity can disclose this information without consent of the patient, such as for treatment (getting a consultation from a specialist), payment (billing the insurance company), for public health activities (such as COVID-19 infection) or due to a court order. This paper will address a covered entity's obligation to protect or disclose PHI under the public health activities exception of HIPAA.[10]

III. Information protected by HIPAA

Protected Health Information is defined as "individually identifiable health information[11]" which means any health information that could identify an individual.

[8] 45 CFR 164.524
[9] Sec. 181.202
[10] 45 C.F.R §164.512(b)(1)(i), available at https://www.law.cornell.edu/cfr/text/45/164.512
[11] 45 C.F.R §160.103, available at https://www.law.cornell.edu/cfr/text/45/160.103

This information is not limited to an individual's name or social security number, but any information that could identify them. This may include:

(1) Written, verbal, or electronic health information

(2) An address or location

(3) Information regarding a patient over age 90

(4) Information that identifies an individual based on a specific characteristic

(5) Any information in a health record such as:

- Lab results, including test results
- Billing information
- Medical Chart information
- Photographs of before and after surgery

Examples of PHI include:

(1) Mr. Smith went to see Dr. Jones

(2) Someone with a face tattoo that reads "My mom is awesome" was treated for COVID-19

(3) I used to be the dental hygienist for our manager and she had enamel erosion

(4) A man on Hialeah Rd. has tuberculosis (and only 3 people live on Hialeah Rd.)

(5) Mrs. Williams had a staph infection on her leg

HIPAA requires covered entities to safeguard PHI, meaning that they are not permitted to disclose it to anyone without the consent of the patient except in accordance with the law.[12] Confusion often arises when someone other than a healthcare provider discloses health information. If your neighbor tells you that Mrs. Williams had a staph infection and the neighbor is not a healthcare provider who

[12] Disclosing to a public health authority is in accordance with the law. See 45 C.F.R §164.512(b)(1)(i), available at https://www.law.cornell.edu/cfr/text/45/164.512

treated Mrs. Williams and did not obtain that information in the course of her job, it's not a violation under HIPAA or Texas law; it's mere gossip.

IV. The Public Health Activities Exception

HIPAA allows[13] covered entities to disclose PHI for the purpose of public health activities, including: a disclosure to a public health authority for the purpose of controlling disease; public health investigations and public health interventions, including the reporting of disease; vital events such as death, child abuse; or a disclosure to another individual who has been exposed to a communicable disease or may be at risk of contracting or spreading a disease, provided that the covered entity is authorized by law to notify that individual.[14] Most people are familiar with the public health activities exception in the case of child abuse or when it comes to notifying a current or former sexual partner of a sexually transmitted disease. In the face of a pandemic such as COVID-19, the public health activities exception allows covered entities to disclose PHI to public health authorities or other government actors so that they can analyze and control a communicable disease.

HIPAA *generally* requires that covered entities follow the "minimum necessary" standard[15] which states:

> *Standard: Minimum necessary - Minimum necessary applies. When using or disclosing [PHI] … a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.*[16]

[13] HIPAA states that the covered entity may disclose PHI without violating HIPAA, but the covered entity is not required to disclose it, unless there is a judicial action which compels them to do so.
[14] 45 C.F.R § 164.512(b), available at: https://www.law.cornell.edu/cfr/text/45/164.512
[15] The minimum necessary standard in 45 C.F.R. § 164.502 does not apply to disclosures of PHI for the purposes of treatment, to the patient, and other necessary means such as healthcare operations.
[16] 45 C.F.R. § 164.502(b) available at https://www.law.cornell.edu/cfr/text/45/164.502

One example of using the minimum necessary standard is when a provider calls to leave a message for someone on their answering machine. Instead of saying "Hi Mr. Carter, we got your test results back and you have syphilis," the minimum necessary standard requires the provider to say "Mr. Carter, this is Sally from Dr. Holt's office. Please give us a call at 555-1234" instead. This is the minimum necessary amount of information to achieve the intended goal of communicating test results with the patient.

When it comes to disclosures for the purpose of public health activities, we look to the state law to determine what information may be disclosed to the local, state or federal authorities for the purposes of public health activities related to communicable diseases. More detailed information on this is below in Section VII.

V. Texas Laws Related to Disclosure for Communicable Disease

Under Texas law, certain covered entities are ***required*** to disclose information to a public health authority related to the existence of a communicable disease,[17] including the name, age, address, and occupation of the patient.[18] However, Texas mandates that these disclosures be kept confidential and that medical or epidemiological information be released only for the following purposes:

- for statistical purposes if released in a manner that prevents the identification of any person
- to medical personnel treating the individual
- to appropriate state agencies in this state or another state
- to a health authority or local health department
- under state or federal law that expressly authorizes the disclosure of this information
- to appropriate federal agencies, such as the Centers for Disease Control and Prevention

[17] Note that this is different than HIPAA, meaning that Texas covered entities must disclose certain information to the public health authority

[18] Texas Health and Safety Code § 81.041 et seq., available at https://statutes.capitol.texas.gov/Docs/HS/pdf/HS.81.pdf

- to medical personnel to the extent necessary in a medical emergency to protect the health or life of the person identified in the information

VI. What the Public Health Authority Does with Your Information

If a covered entity discloses information to a public health authority for the purpose of controlling the spread of a communicable disease, the information will likely include the name, age, gender, and occupation of the patient, along with health information. This is the minimum necessary information that allows the public health authority in the area to gather relevant information for the public, monitor the spread of disease, and create measures to control it.[19] The covered entity may disclose more information than the above, if relevant, without violating HIPAA or Texas law. It is important to understand that a federal public health authority has an obligation to safeguard PHI to the same extent as a covered entity by not disclosing it to any individual or entity that is not on a "need to know" basis. In Texas, a governmental unit, including a public health authority, is considered a covered entity under the TMRPA and also has the obligation to comply with HIPAA.[20]

Typically, the public health authority will gather PHI from covered entities and provide aggregated data by geographic region, age, or other information that is helpful to determine those who may be most affected by a pandemic. The purpose of this aggregated data is to assist the public in understanding which individuals may be most vulnerable and how to prevent the infection from spreading to others.[21] This aggregated data does not identify an individual, so it is not considered PHI.

[19] https://www.cdc.gov/publichealthgateway/publichealthservices/essentialhealthservices.html
[20] Texas Health and Safety Code §181.001(b), available at https://statutes.capitol.texas.gov/Docs/HS/pdf/HS.181.pdf
[21] https://www.cdc.gov/eis/field-epi-manual/chapters/collecting-data.html

The public health activities exception under HIPAA does not expressly contemplate that the public health authority will re-disclose the information to an individual or entity uninvolved in the public health activity of controlling the spread of a communicable disease. The public health authority may, however, choose to disclose the minimum necessary information to the media for the purpose of informing and educating the public.[22] The reason for this is to control the spread of the disease by informing the general public of a risk to their health and safety as it relates to a communicable disease in their geographical location or in areas where they have traveled. This information may be presented in a statement such as "Health Clinic in Forrest County tested 14 patients for COVID-19 this week and 7 tested positive. Two of these patients, ages 57 and 62 years old have been hospitalized." There may be instances when giving information to the media could identify an individual, such as "a 45-year-old female has tested positive for COVID-19 in Loving County, Texas." Loving County has a population of 134 people, so it would be easy to identify which individual in that county was ill. In the case of Loving County, the information may be limited to simply the fact that an individual in the tri-county area tested positive in order to safeguard the identity of the patient.

VII. When the Minimum Necessary Standard Does Not Apply

The Centers for Disease Control and Prevention (CDC)[23] and the state of Texas have declared COVID-19 to be a "high consequence communicable disease."[24] This declaration allows for the following "medical or epidemiological" information to be released to an appropriate federal agency:

(1) the name, address, sex, race, and occupation of the person;

---

[22] https://www.cdc.gov/publichealthgateway/publichealthservices/essentialhealthservices.html, Accessed March 12, 2020

[23] https://www.cdc.gov/coronavirus/2019-ncov/summary.html accessed March 12, 2020

[24] This is the standard set out by Chapter 81 of the Texas Health and Safety Code, available at https://statutes.capitol.texas.gov/Docs/HS/pdf/HS.81.pdf

(2) the date of the onset of the health condition;
(3) the probable source of infection or exposure; and
(4) other requested information relating to the case or suspected case of the infection."[25]

As it relates to a disclosure for this purpose, the patient's PHI is still not being given to the general public, but solely to a federal agency for the purposes of public health activities.

VIII. What Are the Obligations of Employers?

Employers are required to follow applicable state and federal laws relating to the safeguarding of health information. Some of these laws include the Employee Retirement Income Security Act (ERISA),[26] the Americans with Disabilities Act (ADA),[27] and the Family Medical Leave Act (FMLA).[28] These Acts prohibit employers from disclosing health information to others in the workplace unless it is necessary. For example, the plan administrator of a health plan would necessarily need access to healthcare claims as provided for under ERISA; a supervisor would need to know of a disability in order to provide accommodations under the ADA; and the payroll department would need to know about medical leave under FMLA, since it allows for leave without pay. When it comes to communicable diseases, the law has expressly prohibited the disclosure of this information to others in the workforce under the protections of the ADA, unless necessary for an accommodation. It is also illegal for employers to retaliate against employees for having a communicable disease, or for needing protections under these laws.

In addition, the Occupational Safety and Health Act of 1970 was passed "to assure safe and healthful working conditions for working men and women…" which is

[25] Texas Health and Safety Code § 81, available at https://statutes.capitol.texas.gov/Docs/HS/pdf/HS.81.pdf
[26] 29 USC § 1001 et seq
[27] 29 CFR § 1630 et seq
[28] 29 USC § 2601 et seq

difficult to guarantee during a pandemic. In short, the employment laws in the United States do not contemplate the current situation business owners are dealing with by having to balance both health information privacy under HIPAA, ERISA, ADA, and FMLA, and a safe and healthful workplace as required under OSHA. With COVID-19, employers will want to warn their staff of a potential exposure to the disease, but need to remain compliant with the law. Thus, the best way for employers to handle an exposure of COVID-19 in the workplace is to inform staff that an individual was exposed to the disease. This achieves the goal of ensuring a safe and healthful workplace, does not identify any individual who may have a communicable disease, and is the minimum necessary to achieve the goal of warning other staff members.

FAQs

Q: My child's school district told us that a teacher test positive for COVID-19. Why is nobody telling me what school it was in, or what grade that person taught?

A: This information is PHI and the minimum necessary standard applies here. The school district is considered a covered entity in Texas and has to follow HIPAA. The district has informed your family that a teacher tested positive, which should be enough information for you to make decisions regarding the spread of the disease and your potential risk. While it is frustrating, telling you what grade the individual teaches could identify the teacher in violation of HIPAA.

Q: I have HIV and am at risk of contracting COVID-19. Will people find out my HIV status through the news if I end up getting COVID-19?

A: No. Under the minimum necessary standard, a public health authority may disclose to a media outlet that an immunocompromised individual tested positive, but should not indicate what condition caused the lowered immune system because that is not necessary information to prevent the control or spread of the disease. Stating that immunocompromised individuals are at a higher risk of infection or that those individuals may have more severe symptoms falls under information and education of the public.

Q: What if I die? Will people find out I died of COVID-19?

A: Maybe. Your PHI remains protected until fifty (50) years after your death,[29] so a covered entity (including a public health authority) cannot disclose your name to the public or any other individual who does not have authority to obtain the information while you are alive. A covered entity may, however, disclose your PHI to individuals you have given authority to such as a personal representative or the executor of your estate.[30]

Q: I am an attorney that falls under the definition of covered entity in Texas. If a client tests positive for COVID-19, do I have to give the public health authority my client information?

[29] 45 C.F.R. §160.103, definition of "Protected Health Information," available at: https://www.law.cornell.edu/cfr/text/45/160.103

[30] 45 C.F.R. §164.502(g)(4), available at https://www.law.cornell.edu/cfr/text/45/164.502

A: No. You are not considered a covered entity required to report a communicable disease.[31]

Q: I am an immigration attorney. If I test positive for COVID-19, do I have to give the public health authority my client list? I am concerned that they may use that information to deport a client.

A: No. The healthcare provider treating you may request "medical or epidemiological information… relating to the case or suspected case of the infection" as stated in Texas Health and Safety Code § 81(c-3).[32] Note that this does not include or exclude individuals with whom you may have been in close contact. However, you have a separate ethical obligation to safeguard client information, and those obligations are not automatically removed during a public health emergency. In the event you are asked to provide your client list, seek guidance from the State Bar of Texas Ethics Line.

Q: How will I know what information about my health has been disclosed to a public health authority?

A: You have a right under HIPAA to request what is called an "accounting of disclosures"[33] from your healthcare provider. This is a log of disclosures of your PHI to an individual or entity by your provider, what information was disclosed, when it was disclosed, to whom it was disclosed, and a brief description of the purpose for which it was disclosed.

Q: I believe that my PHI was improperly disclosed in violation of HIPAA. I want to sue my healthcare provider for violating HIPAA.

A: The law does not allow you to sue your provider for HIPAA violations. You may, however, file a complaint related to the violation with the Office of Civil Rights online at https://www.hhs.gov/hipaa/filing-a-complaint/index.html

[31] Persons required to report are listed in the Texas Health and Safety Code § 81.042, Available at https://statutes.capitol.texas.gov/Docs/HS/pdf/HS.81.pdf

[32] Available at https://statutes.capitol.texas.gov/Docs/HS/pdf/HS.81.pdf

[33] 45 C.F.R. § 164.528, available at: https://www.law.cornell.edu/cfr/text/45/164.528

Attachment A – HIPAA Basics

I. Obligations of Attorneys

As a covered entity under Texas law, attorneys need to implement the same types of administrative, physical and technical safeguards that covered entities need to implement under federal law. Many attorneys still maintain full paper files, while others have a hybrid of both paper and electronic files or fully electronic files, depending on their practice type. When considering the types of safeguards your practice has, consider whether there are policies and procedures to maintain the confidentiality of all your client files, not just the files that contain PHI. Attorneys may need to upgrade computer systems, encrypt files, or put physical security in place to maintain the confidentiality and security of this information.

II. Required Safeguards

All covered entities are required to develop, implement and enforce safeguards for the protection, use and disclosure of health information. Below is basic information related to each of these safeguards:

a. **Administrative safeguards**[34] are typically policies and procedures related to the protection, use and disclosure of PHI. These may include policies related to security measures, disciplinary actions for employees and contractors who do not comply with protocols, or internal requirements for business associates.

b. **Physical safeguards**[35] are typically physical measures related to the protection of office space, physical files, equipment, and other similar measures. These may include policies and procedures related to when information needs to be locked in a file cabinet, when or if a security camera is installed, and procedures for the protection of PHI in the event of fire, flood, or other hazards.

c. **Technical safeguards**[36] are typically the security measures taken to protect electronic protected health information and control access to it, along with the policies and procedures associated with these measures. These may include items such as end-to-end encryption, HIPAA compliant

[34] 45 CFR § 164.308
[35] 45 CFR § 164.310
[36] 45 CFR § 164.312

server storage, and the use of unique user names and passwords on all systems.

III. Authorized and Unauthorized Disclosures of Information

The purpose of maintaining the administrative, physical and technical safeguards is not to restrict the flow of information necessary to treat patients, but to prevent the use and disclosure of PHI to individuals and entities that have not been expressly authorized by the patient. There are some broad exceptions to such express authorization, including exceptions for the purposes of treatment, payment and healthcare operations. Covered entities may disclose PHI for the purpose of treatment, such as to share information with other providers in a collaborative environment. PHI may be disclosed by a covered entity for the purpose of payment, such as to file claims with an insurance company. Covered entities may also use PHI for healthcare operations, such as to analyze data quality. Attorneys who are covered entities may also fall under these exceptions. For example, a personal injury attorney may disclose information related to payment without an express authorization from a client, so that the client's medical bills can be paid.

a. **Access to Health Information.** Individuals and their personal representatives have the right to access their health information, with very few exceptions.[37] In order to obtain copies of medical records, patients should request the information in writing, and be prepared to pay a reasonable fee[38]

b. **Types of HIPAA Violations.** There are three types of HIPAA violations that lead to breaches of PHI within a covered entity: accidental, intentional, and incidental. An accidental violation is exactly what it sounds like – an unintentional disclosure to someone who was not authorized. These can occur even in the best of circumstances due to human error, such as writing a fax number down incorrectly or putting the wrong address on an envelope. Likewise, an intentional violation is also what it sounds like – an intentional disclosure to someone who was not authorized. Some of the most common types of intentional disclosures involve the sale or theft of PHI. The incidental violation gives

[37] Both HIPAA and TMRPA limit the access of psychotherapy notes, and information compiled for use in certain proceedings, such as to report abuse. The federal limitations on this access are detailed in 45 CFR § 164.524, and the Texas limitations on access to mental health records are detailed in Tex. Health & Safety Code § 611.001 et. seq.
[38] The allowable charges for copies of medical records are located in Tex. Admin. Code § 165.2(e)

the greatest confusion to most people, and most commonly involves the unauthorized use or access of information incident to treatment. One is example is a scenario where two providers are discussing treatment with a patient and the patient in the next room overhears the information. This is incident to the treatment of the patient, and is unavoidable. If the treatment providers are speaking loudly to one another from 30 ft away across a clinic, that would be considered intentional and not incidental.

Other types of violations include:

- Failure to provide access to records timely
- Failure to implement appropriate safeguards
- Failure to train
- Failure to obtain reasonable assurances from business associates

c. **Examples of HIPAA Violations and Allowable Disclosures** There is confusion as to when something is or is not a HIPAA violation. While attorneys tend to err on the side of caution and state that any disclosure of PHI is going to be a HIPAA violation, that is not accurate. HIPAA has many exemptions to allow for the flow of information, and to allow for legal processes to move forward.

A breach is when PHI is disclosed: without an authorization; it does not fall under an exception for treatment, payment, or operations; and the information can be used or disclosed by someone without authorization. A complaint related to a violation of HIPAA may be reported to the Office of Civil Rights, and a complaint related to a violation of TMRPA may be reported to the Texas Attorney General.[39] Once a breach has been discovered by a covered entity, it must be disclosed to the individuals whose information was breached, and to the Secretary of HHS.

Some examples of a HIPAA and/or TMRPA violation include:

- Disclosure by a covered entity for a purpose other than treatment, payment, or operations

[39] A breach of HIPAA may be reported at https://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html and a breach of TMRPA may be reported at https://www.texasattorneygeneral.gov/consumer-protection/health-care/patient-privacy

- Disclosure of personal financial information by a covered entity or business associate of a covered entity, such as a result of a computer security hacking incident
- Theft of paper records
- Loss of an unencrypted computer
- Disclosure of mental health records out of compliance with state and federal law
- Disclosure of PHI by a covered entity to law enforcement without a warrant[40]

Some examples of disclosures that are allowable and are therefore not a HIPAA violation include:

- Disclosure by someone other than a covered entity
- Disclosure to a public health authority in compliance with HIPAA or state law[41]
- Disclosure to a patient while another individual is in the room, where the patient does not expressly authorize or object
- Disclosure to or by an employer for the purposes of Workman's Compensation claims
- Disclosures for the purposes of complying with a subpoena
- Disclosures for the purposes of filing a lawsuit related to medical information
- Disclosures by an employer related to providing or maintaining a health plan
- Disclosures by an employer for the purpose of complying with employment laws
- Any other disclosure that falls under an exception to HIPAA and/or TMRPA, including for public health activities.

[40] An example would be a blood test being disclosed to a law enforcement agency, despite the disclosure not being subject to a warrant, and not falling under any other exception.
[41] Texas Health & Safety Code §81

IV. Safeguarding Client Information

a. **Generally.** Even if one does not fall under the definition of a covered entity, all attorneys need to safeguard client files in compliance with ethical rules as well as state and federal laws. Attorneys and law firms that do fall under the definition of a covered entity for the purposes of TMRPA are obligated to (1) train staff, (2) implement and enforce policies related to data privacy, (3) comply with HIPAA as it relates to the use, disclosure and access to PHI, and (4) implement administrative, physical and technical safeguards within their practice.

b. **Covered Entity Clients.** Attorneys who represent clients that fall under the definition of covered entities should advise their clients on how to comply with state and federal laws, including TMRPA and HIPAA. Part of this compliance may include development and implementation of administrative, physical, and technical safeguards similar as detailed above. In addition, these clients should be trained on relevant law, advised to obtain a BAA for business associates, and to obtain cybersecurity insurance in the event of a computer security breach.

c. **PHI in Lawsuits.** Attorneys who represent clients in lawsuits that center around medical information may disclose PHI in pleadings for the purpose of the lawsuit. Examples of these include guardianship proceedings, medical malpractice claims, and personal injury lawsuits. If the lawsuit does not center around medical information, the attorney filing the pleadings should protect the information, which can be achieved by the following methods:[42]

   i. De-identification or redaction of PHI

   ii. Filing the pleadings under seal

   iii. Filing a protective order

Clients will need to provide their attorney with a HIPAA compliant release of information form so that the client's treatment providers can disclose the information

[42] This list is not exhaustive and merely for illustration purposes

for the purpose of a lawsuit.[43] Attorneys should also be aware that mental health and substance abuse records may not be available, even to their client. Finally, attorneys need to be aware that while there is no private right of action under HIPAA, there may be a cause of action under tort, employment, or other laws related to privacy.

[43] A copy of the Texas Attorney General HIPAA authorization form is included with this presentation and can be found here: https://www.texasattorneygeneral.gov/sites/default/files/files/divisions/consumer-protection/hb300-Authorization-Disclose-Health-Info.pdf