



**modivcare**

# HIPAA PRIVACY & SECURITY

(INCLUDING TEXAS MEDICAL PRIVACYLAW)



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

This course will explain our policy regarding the privacy and security of healthcare information in compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Texas Medical Privacy Law.

At the end of the course material, you'll take a quiz that presents hypothetical situations for you to analyze. You must pass the quiz with a score of 80% or above to complete the course.

If you have any questions regarding our privacy practices, please contact ModivCare's Privacy Officer, Jody Kepler, or ModivCare's VP of Privacy, Adam Lovett, at [hipaaofficer@modivcare.com](mailto:hipaaofficer@modivcare.com)

If you have any questions about data security or need to report a potential security incident, [please contact our Chief Information Security Officer, Travis Lansdell, at modivcare@service-now.com](mailto:modivcare@service-now.com)



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## WHAT IS HIPAA?

HIPAA is a far-reaching federal law passed in 1996. HIPAA's primary purpose for ModivCare is:

- **Privacy and security of protected health information (PHI)**
- Only disclosing PHI in appropriate circumstances

## IMPROPER DISCLOSURES

Some examples of improper disclosures of PHI are:

- Posting Members' trip records on social media
- Sending an unencrypted email to a transportation provider discussing a Member complaint
- Employees reading a Member's record "just for fun"
- Marketing a list of Member names

## STATE LAWS

- HIPAA *preempts* state law unless the state law affords greater protection for PHI. We must follow whichever law is more stringent regarding the privacy and security of the information.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## WHO IS SUBJECT TO HIPAA?

**COVERED ENTITIES** include hospitals, insurance companies, and small physician practices.

There are three categories of Covered Entities:

- Healthcare plans
- Health providers
- Clearinghouses of health information



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## WHO ELSE IS SUBJECT TO HIPAA?

### BUSINESS ASSOCIATES

- A Business Associate creates, receives, maintains or transmits PHI on behalf of a Covered Entity to carry out healthcare activities and functions
- ModivCare is a Business Associate of health plans, state Medicaid agencies and other Covered Entities with whom we contract
- Business Associates must:
  1. Provide written (contractual) assurance they will comply with HIPAA requirements in a Business Associate Agreement (BAA)
  2. Comply with all HIPAA regulations requiring safeguards for the security of PHI
  3. Comply with certain HIPAA regulations pertaining to the privacy of the information

### SECURITY

HITECH (effective in 2010) made the HIPAA Security Rule directly applicable to Business Associates.

### PRIVACY

The Omnibus Rule (effective in 2013) made certain portions of the HIPAA Privacy Rule directly applicable to Business Associates.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## WHO ELSE IS SUBJECT TO HIPAA?

### BUSINESS ASSOCIATE SUBCONTRACTORS

If a Business Associate uses one or more subcontractors to perform certain functions or activities involving PHI, HIPAA requires agreements between that Business Associate and their subcontractors.

- Subcontractors are contractually obligated to comply with HIPAA requirements.
- Subcontractors are subject to HIPAA requirements separate and apart from their contractual agreements with Business Associates.
- **Transportation providers and technology vendors** that create, receive, maintain, or transmit PHI on behalf ModivCare are considered Business Associate Subcontractors and are therefore subject to HIPAA requirements.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

PHI is information identifying an individual that relates to one of the following:

- The past, present, or future physical or mental health condition of an individual
- Providing healthcare to an individual
- Payment for healthcare of an individual

**Any identifiable information about ModivCare's Members is treated as PHI under HIPAA.**

The HIPAA Privacy Rule covers PHI in all forms (printed, spoken, and electronic), while the Security Rule covers only *electronic* PHI.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## HIPAA PRIVACY

ModivCare may use or disclose an individual's PHI:

- To communicate directly with the individual about his/her PHI
- With the individual's written authorization
- Without the individual's authorization for **treatment, payment, and health care operations**

When using, disclosing or requesting PHI, we must make reasonable efforts to limit our use, disclosure or request to the **minimum necessary** to accomplish the intended purpose of the use, disclosure or request.

## TREATMENT, PAYMENT, AND HEALTHCARE OPERATIONS (TPO)

Applicable state laws could require written consent for the use and disclosure of PHI for TPO purposes.

## MINIMUM NECESSARY

- You are required to limit your information requests to the minimum necessary PHI for the relevant work task.
- Transportation providers and IT vendors must only be provided the minimum necessary PHI to provide services to Members.





# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## REASONABLE SAFEGUARDS

ModivCare must use **reasonable safeguards** to protect the confidentiality of PHI.

Reasonable safeguards include:

- Not discussing PHI outside of ModivCare's offices or your designated work from home space
- Not naming the individual whose PHI is being discussed when feasible
- Keeping PHI secure at your workstations
- Isolating and locking filing cabinets that contain printed PHI
- Equipping computers with password-protected screensavers



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## USING PHI FOR MARKETING

The HIPAA Privacy Rule gives individuals important controls over the use and disclosure of their PHI for marketing purposes.

**ModivCare may not disclose PHI for marketing purposes without the Member's express, written authorization. The Privacy Rule defines "marketing" as making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.**

The Privacy Rule carves out exceptions to the definition of marketing under the following three categories:

- 1) If a communication is made to describe a health-related product or service;
- 2) If a communication is made for treatment of the individual; and
- 3) If a communication is for case management, care coordination for the individual, or to direct, or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## USING PHI FOR MARKETING

### SALE OF PHI

The Omnibus Rule prohibits ModivCare from selling PHI without first obtaining authorization. The authorization must state that the disclosure will result in compensation. The sale of PHI does not include disclosures:

- For public health purposes
- For research purposes
- For treatment and payment purposes
- To a Business Associate
- To an individual when requested under the Privacy Rule
- Required by law
- For any other purpose under the Privacy Rule with no compensation other than a cost-based fee to prepare and transmit the PHI



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## HIPAA SECURITY

**Security Rule** addresses the creation, receipt, maintenance, and transmission of **electronic PHI** by covered entities and business associates. The primary goals are:

- To maintain the confidentiality of stored and transmitted electronic PHI
- To protect electronic PHI from unauthorized creation, modification, and deletion
- To ensure that electronic PHI is available to authorized individuals or entities when needed

Required Security safeguards categorized for compliance are:

- **Administrative**
- **Physical**
- **Technical**



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## ADMINISTRATIVE SAFEGUARDS

- **Security Officer** for the development and implementation of security policies.

**ModivCare's Chief Information Security Officer is Travis Lansdell.**

- **Workforce Security** plan for granting employees varying levels of access to PHI
- **Contingency Plan** for responding to system emergencies and natural disasters
- **Business Associate Contracts** to protect the confidentiality of PHI exchange
- **Termination Procedures** to prevent a terminated employee from accessing PHI



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## PHYSICAL SAFEGUARDS

Physical safeguards include:

- **Facility Access Controls** that allow only authorized access to locations where PHI is stored
- **Workstation Use Procedures** for PHI displayed on computer screens
- **Workstation Security** includes secured rooms, curtains, partitions, and user IDs and passwords for workstations on which PHI is processed
- **Device and Media Controls** for the handling of computer hardware and software, including proper disposal and storage



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## TECHNICAL SAFEGUARDS

The Security Rule requires that we implement technical safeguards for electronic PHI, including:

- **Access Controls** limiting access to PHI on a need-to-know basis, based on roles and context
- **Audit Controls** for recording and examining system activity to eliminate unnecessary access to PHI
- **Person or Entity Authentication** to ensure only authorized access to PHI
- **Transmission Security** to protect PHI during transmission over electronic networks



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## HANDLING PHI

Guidelines when handling PHI:

- Access PHI only to the extent necessary to perform job-related functions
- Destroy PHI when no longer needed
- Verify the proper receipt of transmitted PHI
- Secure work areas with locks and passwords
- Take special precautions while working in the field or at home to ensure security of PHI





# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## SECURITY BREACH AND HIPAA INCIDENT REPORTING

If there is a security **breach** involving unsecured PHI:

- **Notice** must be given to **affected individuals**
- If the breach affects 500 or more individuals, the responsible entity is required to notify the **government and media**.

All **suspected breaches** or potential **HIPAA/privacy** incidents should be reported to the **HIPAA Privacy Officer, Jody Kepler**, and **VP of Privacy, Adam Lovett**, at [hipaaofficer@modivcare.com](mailto:hipaaofficer@modivcare.com) **immediately** so that they can make sure the appropriate notifications are made within the timeframes required by law.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## SECURITY BREACH

### WHEN A BREACH REQUIRES NOTICE

A **breach** is "the unauthorized acquisition, access, use, or disclosure" of an individual's PHI.

A disclosure is not a breach if it was:

- Within the course and scope of employment, and did not result in further disclosure
- Inadvertent by an authorized individual to another authorized individual at the same covered entity and not further used or disclosed
- Made to someone who would not reasonably have been able to retain the information

If the acquisition, access, use, or disclosure does not qualify for an exception, there is a presumption of a breach **unless** the responsible entity demonstrates a low probability the PHI has been compromised based upon a **risk assessment**.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## SECURITY BREACH

### NOTICE TO COVERED ENTITY

A Business Associate must notify the Covered Entity when it discovers a breach no later than 60 days from the discovery of the breach (or shorter period as stipulated in the applicable BAA).

### NOTICE TO AFFECTED INDIVIDUALS

Notice must be:

- Issued no more than 60 days after the breach
- Made by letter or by email

If the contact information for the affected individuals is unavailable, other forms of notice may be used.

### BREACH AFFECTING 500 OR MORE

If breach affects 500 or more individuals, notice must be provided to the U.S. Department of Health and Human Services and to certain media outlets. We must also follow any applicable state breach notification laws.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## PHI RIGHTS OF INDIVIDUALS

In addition to the previous discussion, individuals have rights over the use and disclosure of their PHI. Determining whether these rights apply in a particular situation is a function of ModivCare's Legal Department and HIPAA Officers:

- Covered Entities must abide by an individual's request not to divulge PHI if he/she is paying for the full service cost
- Individuals are entitled to **copies of medical records** that a Covered Entity keeps electronically
- Individuals have the right to request that a Covered Entity **correct any inaccurate PHI**
- Covered Entities **maintaining electronic health records** must provide an accounting of all PHI disclosures during the prior **three years**, upon request



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## RECORD RETENTION

Covered Entities and Business Associates must retain all **compliance documentation** relating to PHI for a period of at least **six years** from the date of its creation or the date when it was last in effect, including without limitation, the following:

- Policies and procedures governing the use and disclosure of PHI
- Training provided to the Covered Entity/Business Associate's workforce
- The Covered Entity/Business Associate's designated privacy officials including contact information
- Complaints to the Covered Entity/Business Associate and their disposition
- Authorizations for uses and disclosures of PHI
- Business Associate Agreements
- Accountings of requests for disclosure of individuals' PHI
- Agreements to restrict uses or disclosures of individuals' PHI



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## ENFORCEMENT

Penalties for failure to comply with HIPAA:

- **Civil fines range from \$100 to \$50,000** for each violation, varying based upon culpability, up to **\$1.5 million** per year for willful neglect, not corrected
- **Criminal penalties** for a basic offense are fines of up to **\$50,000** and/or **imprisonment for up to one year**
- Criminal penalties for offenses under **false pretenses** are fines of up to **\$100,000** and/or **imprisonment for up to five years**
- Criminal penalties for an offense with intent to use PHI for **commercial advantage** are fines of up to **\$250,000** and/or **imprisonment for up to ten years**



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## TEXAS MEDICAL PRIVACY LAW

Texas law imposes even stricter requirements than HIPAA. Requirements on Covered Entities include:

- **Records requests:** must provide electronic health records to Members within 15 business days of request
- **Notice:** must provide notice if PHI is subject to electronic disclosure
- **Disclosures:** must use a [form provided by the state Attorney General](#)
- **Security breaches:** must notify all affected individuals as soon as possible

Covered Entities face potential **penalties** under Texas law for wrongful disclosure of PHI.



# HIPAA PRIVACY & SECURITY (INCLUDING TEXAS MEDICAL PRIVACY LAW)

## TEXAS MEDICAL PRIVACY LAW COVERED

### ENTITIES

Texas law defines a “Covered Entity” as any individual, business, or organization that:

- Engages in assembling, collecting, analyzing, storing, or transmitting PHI
- Comes into the possession of PHI
- Obtains or stores PHI
- Is an employee, agent or contractor of a person who performs one of the functions described above

### PENALTIES

Texas law provides the following civil penalties for each year a violation exists:

- Up to **\$5,000** for each violation committed **negligently**
- Up to **\$25,000** for each violation committed **knowingly**
- Up to **\$250,000** if the PHI was used for **financial gain**
- Up to **\$1.5 million** if the court finds a **pattern or practice of violations**

**Covered Entities may also be fined \$100 per person per day — up to \$250,000 per incident — for failure to notify those affected by a security breach.**