Texas HB 300

ProAssurance®

Treated Fairly

HB 300: Background

- Texas House Research Organizational Bill Analysis for HB 300 shows state legislators believed HIPAA did not provide enough protection for private health information (PHI) in light of increased use of electronic records
- Compliance with HB 300 is “above and beyond” HIPAA’s requirements

Evolution of HB 300

- HIPAA passed in 1996
- Originally, HIPAA only directly impacted certain "covered entities":
  - Healthcare providers (e.g., hospitals and physicians)
  - Healthcare plans (e.g., HMOs and self-insured health plans)
  - Healthcare clearinghouses (e.g., billing services and repricing companies)
- Under HITECH and final rules, many provisions now apply to a broad range of "business associates," including those that *maintain* PHI

HB 300: Broader Definition of Covered Entity Than Under HIPAA

Includes any person who:

- 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 PHI, including 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

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

HB 300: Broader Definition of Covered Entity Than Under HIPAA

Includes any person who:

- Comes into *possession* of PHI
- Obtains or stores PHI
- Is an employee, agent, or contractor of a "covered entity" insofar as the employee, agent or contractor creates, receives, obtains, maintains, uses or transmits PHI

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

Potential Scope of HB 300 as Written

- Sports teams
- Camps
- Someone receiving individual-identifying health information via text or social media
- Document shredding companies
- Any other vendor who would touch PHI

Exemptions to "Covered Entity"

- Covered entity as defined by Section 602.001 of the Insurance Code
- Entity established under Art. 5.76-3 of the Insurance Code
- Financial Institutions or others engaged in processing payments (but only to the extent they are engaged in the enumerated financial activities)
- Non-profit agencies, even if they pay for healthcare or prescription drugs for indigents, if their primary business is not providing healthcare or reimbursement for healthcare

Exemptions to "Covered Entity" (Continued)

- Workers' compensation insurance
- Employee benefit plans
- American Red Cross (regarding duties to provide biomedical services, disaster relief, disaster communication, or emergency leave verification for military)
- Information and records relating to offenders with mental impairments
- Educational records covered by 20 U.S.C. Sections 1232g and 1232g(a)(4)(B)(iv)
- Actions in connection with crime victim compensation

Tex. Health & Safety Code §181.054 -.059

Training Requirements

- Covered entities must now provide ongoing, customized training for employees, on both federal and state PHI laws, within 60 days of hire and at least once every two years
- No specifics about length or required curriculum content

Tex. Health & Safety Code §181.101

Training Requirements (Continued)

- Training programs should relate to the company's "particular course of business" and the individual employee's scope of employment in regards to PHI
  - For instance, training requirements could possibly be less extensive for those who do not routinely deal with PHI Some commentators question whether any training would be required for employees with no access, as not relative to their scope of employment
  - These issues are currently unresolved

Training Requirements (Continued)

- Covered entities must retain a signed statement verifying the employee's attendance at the training program
- Such record may be signed electronically or in writing, but must be maintained

Tex. Health & Safety Code §181.101(d)

Patient Access to Electronic Health Records

- "Health care providers" as defined by HIPAA, and utilizing an electronic health records system capable of fulfilling a request for a person's electronic health record (EHR), *must* provide the record to the patient in electronic form within 15 business days of receiving a written request (unless the person agrees to accept it in another form). *Note: Does not apply to other "covered entities" under HB 300*

Tex. Health and Safety Code, §181.102(a)

  - This requirement supersedes the 30 days allowed under HIPAA
  - Access to records is not required if not required under 42 C.F.R. Section 164.524
  - The executive commissioner may recommend a standard electronic format

HB 300: Consumer Information Website

- The attorney general is to maintain a website providing:
  - Information on consumer's privacy rights related to PHI under federal and state law
  - A list of state agencies that regulate covered entities
  - Detailed information on each agency's complaint enforcement process
  - Agency contact information for reporting a HB 300 violation

Tex. Health and Safety Code, §181.103

Prohibited Acts

- A person may not reidentify or try to reidentify a person's PHI without consent or authorization if required under HB 300, or other state or federal law

Tex. Health and Safety Code, §181.151

Prohibited Acts (Continued)

- Marketing
  - Need "clear and unambiguous" permission, in written or electronic form, to use or disclose PHI for marketing communications, unless one of the following exceptions apply:
    - Face-to-face communication by covered entity to an individual
    - A promotional gift of nominal value provided by covered entity
    - Communication is necessary for administering a patient assistance program or other prescription drug savings or discount program
    - The communication is made at the individual's oral request

Tex. Health and Safety Code, §181.152(a)

Prohibited Acts (Continued)

- Marketing (continued)
  - If a written marketing communication is made through the mail, it must be sent in an envelope showing only names and addresses of sender and recipient, and must:
    - state the name and toll-free number of the entity sending the marketing communication; and
    - explain the right to have the recipient's name removed from mailing list
  - If requested to remove a person from the mailing list, the name shall be removed within 45 days from receipt of the request

Tex. Health and Safety Code, §181.152(b) & (c)

Prohibited Acts (Continued)

- Marketing (continued)
  - If the marketing communication is made pursuant to oral request, there must be “clear and unambiguous” oral permission for the use or disclosure of the PHI
    - The communication must be limited to the scope of the oral permission
    - Any further marketing communication must comply with the marketing requirements of HB 300

Tex. Health and Safety Code, §181.152(d)

Prohibited Acts (Continued)

- Sale of PHI
  - May not disclose PHI in exchange for direct or indirect remuneration. *Exceptions*:
    - To another covered entity for treatment, payment, health care operations, or insurance or HMO functions under the Insurance Code
    - As otherwise authorized or required by state or federal law

Tex. Health and Safety Code, §181.153(a)

Prohibited Acts (Continued)

- Sale of PHI (continued)
  - The direct or indirect remuneration to a covered entity who discloses information for an insurance or HMO function described in § 602.053 of the Insurance Code may not exceed the reasonable costs of preparing or transmitting the information

Tex. Health and Safety Code, §181.153(b)

HB 300: Additional Required Authorizations

- A covered entity may not **electronically disclose** an individual's protected health information to any person without a **separate** authorization from the individual or the individual's legally authorized representative **for each disclosure.** Authorization is not required if the disclosure is made for the purpose of treatment, payment, health care operations, performance of an insurance or health maintenance organization function, or as otherwise authorized or required by state or federal law
- May be in written or electronic form; oral authorization is permitted if documented in writing by the covered entity

Tex. Health & Safety Code §181.154(b) and (c)

Electronic Disclosure Notice

- Covered entities that create or receive PHI for an individual must provide **notice** to that individual if his/her PHI is subject to electronic disclosure
- General Notice may be provided by:
  - posting a written notice in the covered entity's place of business;
  - posting a notice on their Internet website; or
  - posting a notice in any other place where individuals subject to the notice are likely to see it

Tex. Health & Safety Code §181.154(a)

Sample Notice

Texas Health and Safety Code Sec. 181.154

NOTICE AND AUTHORIZATION FOR ELECTRONIC DISCLOSURE OF PROTECTED HEALTH INFORMATION;

(a) A covered entity shall provide notice to an individual for whom the covered entity creates or receives protected health information if the individual's protected health information is subject to electronic disclosure

(b) A covered entity may not electronically disclose an individual's protected health information to any person without a separate authorization from the individual or the individual's legally authorized representative for each disclosure. An authorization for disclosure under this subsection may be made in written or electronic form, or in oral form if it is documented in writing by the covered entity

(c) The authorization for electronic disclosure of protected health information described is not required if the disclosure is made:

(1) to another covered entity for the purpose of:

(A) treatment;

(B) payment;

(C) health care operations; or

(D) performing an insurance or health maintenance organization function; or as otherwise authorized or required by state or federal law

Attorney General's Standard Authorization

AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION

Developed for Texas Health & Safety Code § 181.154(d)
effective January 1, 2013

Please read this entire form before signing and complete all the sections that apply to your decisions relating to the disclosure of protected health information. Covered entities as that term is defined by HIPAA and Texas Health & Safety Code § 181.001 must obtain a signed authorization from the individual or the individual's legally authorized representative to electronically disclose that individual's protected health information. Authorization is not required for disclosures related to treatment, payment, health care operations, performing an insurance or health maintenance organization function, or as may be otherwise authorized by law. **Covered entities may use this form or any other form that complies with HIPAA, the Texas Medical Privacy Act, and other applicable laws.** Individuals cannot be denied treatment based on a failure to sign this authorization form, and a refusal to sign this form will not affect the payment, enrollment, or eligibility for benefits.

NAME OF PATIENT OR INDIVIDUAL

Last First Middle

OTHER NAME(S) USED

DATE OF BIRTH Month Day Year

ADDRESS

CITY **STATE** **ZIP**

PHONE ( ) **ALT. PHONE** ( )

EMAIL ADDRESS (Optional):

I AUTHORIZE THE FOLLOWING TO DISCLOSE THE INDIVIDUAL'S PROTECTED HEALTH INFORMATION:

Person/Organization Name
Address
City State Zip Code
Phone ( ) Fax ( )

WHO CAN RECEIVE AND USE THE HEALTH INFORMATION?

Person/Organization Name
Address
City State Zip Code
Phone ( ) Fax ( )

REASON FOR DISCLOSURE
(Choose only one option below)

- ☐ Treatment/Continuing Medical Care
- ☐ Personal Use
- ☐ Billing or Claims
- ☐ Insurance
- ☐ Legal Purposes
- ☐ Disability Determination
- ☐ School
- ☐ Employment
- ☐ Other

WHAT INFORMATION CAN BE DISCLOSED? Complete the following by indicating those items that you want disclosed. The signature of a minor patient is required for the release of some of these items. If all health information is to be released, then check only the first box.

- ☐ **All health information**
- ☐ Physician's Orders
- ☐ Progress Notes
- ☐ Pathology Reports
- ☐ History/Physical Exam
- ☐ Patient Allergies
- ☐ Discharge Summary
- ☐ Billing Information
- ☐ Past/Present Medications
- ☐ Operation Reports
- ☐ Diagnostic Test Reports
- ☐ Radiology Reports & Images
- ☐ Lab Results
- ☐ Consultation Reports
- ☐ EKG/Cardiology Reports
- ☐ Other

Your initials are required to release the following information:

_____Mental Health Records (excluding psychotherapy notes)
_____Drug, Alcohol, or Substance Abuse Records
_____Genetic Information (including Genetic Test Results)
_____HIV/AIDS Test Results/Treatment

EFFECTIVE TIME PERIOD. This authorization is valid until the earlier of the occurrence of the death of the individual, the individual reaching the age of majority, or permission is withdrawn; or the following specific date (optional). Month Day Year

RIGHT TO REVOKE: I understand that I can withdraw my permission at any time by giving written notice stating my intent to revoke this authorization to the person or organization named under "WHO CAN RECEIVE AND USE THE HEALTH INFORMATION." I understand that prior actions taken in reliance on this authorization by entities that had permission to access my health information will not be affected.

SIGNATURE AUTHORIZATION: I have read this form and agree to the uses and disclosures of the information as described. I understand that refusing to sign this form does not stop disclosure of health information that has occurred prior to revocation or that is otherwise permitted by law without my specific authorization or permission, including disclosures to other covered entities as provided by Texas Health & Safety Code § 181.154(c) and/or 45 C.F.R. § 164.506(a)(1). I understand that information disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and may no longer be protected by federal or state privacy laws.

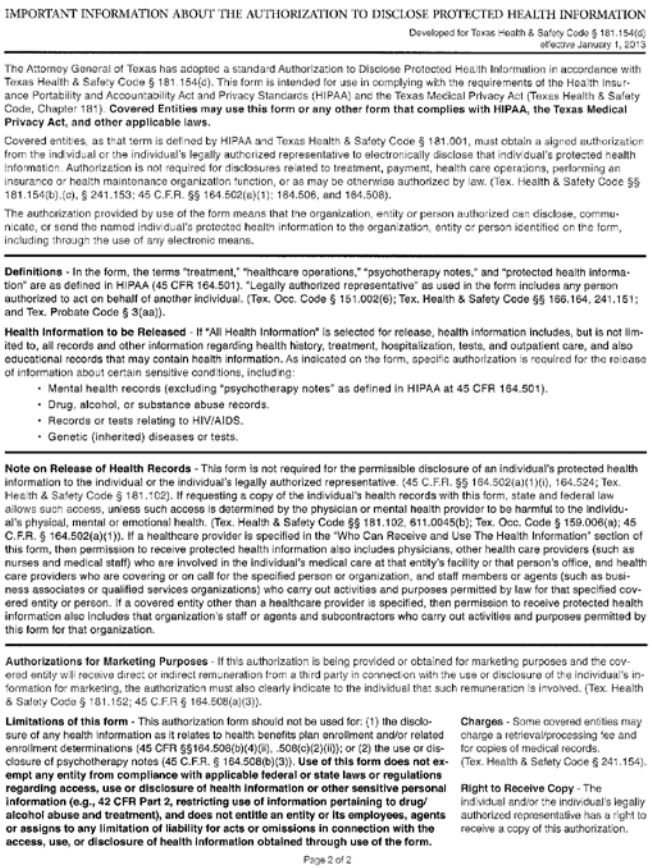
SIGNATURE X _____ _____
Signature of Individual or Individual's Legally Authorized Representative **DATE**

Printed Name of Legally Authorized Representative (if applicable):
If representative, specify relationship to the individual: ☐ Parent of minor ☐ Guardian ☐ Other

A minor individual's signature is required for the release of certain types of information, including for example, the release of information related to certain types of reproductive care, sexually transmitted diseases, and drug, alcohol or substance abuse, and mental health treatment (See, e.g., Tex. Fam. Code § 32.003).

SIGNATURE X _____ _____
Signature of Minor Individual **DATE**

Page 1 of 2



IMPORTANT INFORMATION ABOUT THE AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION

Developed for Texas Health & Safety Code § 181.154(d)
effective January 1, 2013

The Attorney General of Texas has adopted a standard Authorization to Disclose Protected Health Information in accordance with Texas Health & Safety Code § 181.154(d). This form is intended for use in complying with the requirements of the Health Insurance Portability and Accountability Act and Privacy Standards (HIPAA) and the Texas Medical Privacy Act (Texas Health & Safety Code, Chapter 181). **Covered Entities may use this form or any other form that complies with HIPAA, the Texas Medical Privacy Act, and other applicable laws.**

Covered entities, as that term is defined by HIPAA and Texas Health & Safety Code § 181.001, must obtain a signed authorization from the individual or the individual's legally authorized representative to electronically disclose that individual's protected health information. Authorization is not required for disclosures related to treatment, payment, health care operations, performing an insurance or health maintenance organization function, or as may be otherwise authorized by law. (Tex. Health & Safety Code §§ 181.154(b),(c), § 241.153; 45 C.F.R. §§ 164.502(a)(1): 164.506, and 164.508).

The authorization provided by use of the form means that the organization, entity or person authorized can disclose, communicate, or send the named individual's protected health information to the organization, entity or person identified on the form, including through the use of any electronic means.

Definitions - In the form, the terms "treatment," "healthcare operations," "psychotherapy notes," and "protected health information" are as defined in HIPAA (45 CFR 164.501). "Legally authorized representative" as used in the form includes any person authorized to act on behalf of another individual. (Tex. Occ. Code § 151.002(6); Tex. Health & Safety Code §§ 166.164, 241.151; and Tex. Probate Code § 3(aa)).

Health Information to be Released - If "All Health Information" is selected for release, health information includes, but is not limited to, all records and other information regarding health history, treatment, hospitalization, tests, and outpatient care, and also educational records that may contain health information. As indicated on the form, specific authorization is required for the release of information about certain sensitive conditions, including:

- Mental health records (excluding "psychotherapy notes" as defined in HIPAA at 45 CFR 164.501).
- Drug, alcohol, or substance abuse records.
- Records or tests relating to HIV/AIDS.
- Genetic (inherited) diseases or tests.

Note on Release of Health Records - This form is not required for the permissible disclosure of an individual's protected health information to the individual or the individual's legally authorized representative. (45 C.F.R. §§ 164.502(a)(1)(i), 164.524; Tex. Health & Safety Code § 181.102). If requesting a copy of the individual's health records with this form, state and federal law allows such access, unless such access is determined by the physician or mental health provider to be harmful to the individual's physical, mental or emotional health. (Tex. Health & Safety Code §§ 181.102, 611.0045(b); Tex. Occ. Code § 159.006(a); 45 C.F.R. § 164.502(a)(1)). If a healthcare provider is specified in the "Who Can Receive and Use The Health Information" section of this form, then permission to receive protected health information also includes physicians, other health care providers (such as nurses and medical staff) who are involved in the individual's medical care at that entity's facility or that person's office, and health care providers who are covering or on call for the specified person or organization, and staff members or agents (such as business associates or qualified services organizations) who carry out activities and purposes permitted by law for that specified covered entity or person. If a covered entity other than a healthcare provider is specified, then permission to receive protected health information also includes that organization's staff or agents and subcontractors who carry out activities and purposes permitted by this form for that organization.

Authorizations for Marketing Purposes - If this authorization is being provided or obtained for marketing purposes and the covered entity will receive direct or indirect remuneration from a third party in connection with the use or disclosure of the individual's information for marketing, the authorization must also clearly indicate to the individual that such remuneration is involved. (Tex. Health & Safety Code § 181.152; 45 C.F.R § 164.508(a)(3)).

Limitations of this form - This authorization form should not be used for: (1) the disclosure of any health information as it relates to health benefits plan enrollment and/or related enrollment determinations (45 CFR §§164.508(b)(4)(ii), .508(b)(2)(ii)); or (2) the use or disclosure of psychotherapy notes (45 C.F.R. § 164.508(b)(3)). **Use of this form does not exempt any entity from compliance with applicable federal or state laws or regulations regarding access, use or disclosure of health information or other sensitive personal information (e.g., 42 CFR Part 2, restricting use of information pertaining to drug/alcohol abuse and treatment), and does not entitle an entity or its employees, agents or assigns to any limitation of liability for acts or omissions in connection with the access, use, or disclosure of health information obtained through use of the form.**

Charges - Some covered entities may charge a retrieval/processing fee and for copies of medical records. (Tex. Health & Safety Code § 241.154).

Right to Receive Copy - The individual and/or the individual's legally authorized representative has a right to receive a copy of this authorization.

Page 2 of 2

ProAssurance.
Treated Fairly

Attorney General's Standard Authorization (Continued)

- https://www.oag.state.tx.us/newspubs/publications.shtml
- For a PDF copy, click on "Publications" under the Consumer Protection sub-section

Breach Notification Expanded

- Any person conducting business in Texas, who owns or licenses computerized data that includes sensitive personal information (including PHI) must notify Texas residents (or a resident of another state if that state does not have breach notification requirements) of a breach, if that information was acquired or reasonably believed to have been acquired by an unauthorized person
  - A "breach of system security" is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information. It includes encrypted data if the person accessing has a key to decrypt the data
  - An employee or agent's good faith acquisition of the data is not a breach unless the person uses or discloses the sensitive personal information in an unauthorized manner
  - If the affected individual is a resident of another state with breach notification requirements, satisfying that state's requirements is sufficient notification

Tex. Bus. & Comm. Code §521.053

Breach Notification Expanded (Continued)

- The disclosure shall be made as quickly as possible, except when a law enforcement agency has determined that notification would impede an investigation and requested a delay, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system
- Notice may be written notice or electronic (if the electronic notice is provided in accordance with 15 U.S.C. Section 7001)
- Alternate notice provisions exist if the cost of notice will exceed $250,000 or will be to over 500,000 persons, or if the person affected has insufficient contact information

Tex. Bus. & Comm. Code §521.053

Breach Notification Expanded (Continued)

- Notwithstanding the notice provisions, “a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy”
- If more than 10,000 persons are required to be notified at once, consumer reporting agencies, without unreasonable delay, must also be notified of the timing, distribution, and content of the notices

Tex. Bus. & Comm. Code §521.053

Penalties for Disclosure Violations

The state attorney general's office, in addition to injunctive relief, may institute an action for civil penalties for violations, not to exceed:

- $5,000 per violation per year if negligent
- $25,000 per violation per year if knowing or intentional
- $250,000 per violation if knowing or intentional **and** for financial gain
- Pattern or practice of abuse can result in penalties up to $1.5 million annually

Tex. Health & Safety Code §181.201

Penalties for Disclosure Violations (Continued)

The court shall consider several factors in determining the penalty amount:

- Seriousness of the violation, including nature, circumstances, extent, and gravity of the disclosure
- Compliance history
- Whether violation poses a significant risk of harm to the affected person, either financial, reputational, or other harm
- Whether the covered entity was certified by the Texas Health Services Authority when the violation occurred
- Amount necessary to deter in future
- Efforts to correct

Tex. Health & Safety Code §181.201

Penalties for Disclosure Violations (Continued)

- In addition to fines, an individual or facility that is licensed by a Texas agency and who commits a violation is subject to investigation and disciplinary proceedings, including probation or suspension. If there is evidence the violations are egregious and constitute a pattern or practice, the agency may revoke the license or refer to the Attorney General
- A court finding of a pattern or practice of violations also can lead to exclusion from any state-funded health care program

Tex. Health & Safety Code §181.202 and §181.203

Penalties for Disclosure Violations (Continued)

- In defending against an administration or civil penalty, a covered entity can use evidence to show good faith efforts to comply with state law and HIPAA in order to try and mitigate any penalty
- The same factors that determine a civil penalty shall also be considered in any disciplinary action

Tex. Health & Safety Code §181.205

Penalties for Disclosure Violations (Continued)

- Additional penalties exist for failure to notify individuals of a breach
  - No more than $100 per individual for each day the person fails to "take reasonable action to comply"
  - No greater than $250,000 for all individuals owed notification after a single breach

  Tex. Bus. & Com. Code §521.151
- Using a scanning device or re-encoder to access, read, scan, store, or transfer PHI on the magnetic strip of a payment card, without consent and with intent to harm or defraud, is a state jail felony

  Tex. Bus. & Com. Code §522.002

Audits

- The Texas Health and Human Services Commission, in coordination with the Attorney General, Texas Health Services Authority, and the Texas Department of Insurance, may request the U.S. HHS conduct an audit for compliance with HIPAA
- If the commission has evidence of egregious violations that constitute a pattern or practice, the commission can require submission of risk analysis results, or request the licensing agency of a licensed covered entity conduct an audit to determine compliance

Tex. Health & Safety Code §181.206

Practice Suggestions

- Provide and document training programs
- Consider use of encryption for storing or transmitting PHI
- Post notice regarding Texas Medical Records Privacy Act
- Develop and/or update security policies and procedures

Practice Suggestions (Continued)

- Revise policies and procedures regarding patient's access to their electronic medical records to comply with the HB 300 authorization requirements
- Update current business associate agreements to include HB 300 requirements
- Enter into additional business associate agreements with vendors that may now be "covered entities" under HB 300, although mere "conduits" and thus not covered under HIPAA/HITECH

Practice Suggestions (Continued)

- Consider certification by the Texas Health Services Authority (when available)
- Review insurance policies for coverage of HIPAA, HITECH, or HB 300 violations, including all fines, penalties, and defense costs