TEXAS MEDICAL ASSOCIATION

Physicians Caring for Texans

House Committee on Business & Industry
Testimony on House Bill 3746
Submitted by Texas Medical Association
April 13, 2021

Dear Chairman Turner and committee members:

The Texas Medical Association appreciates the opportunity to submit this testimony ***ON*** House Bill 3746. As a nonprofit organization with more than 55,000 physician and medical student members, we have great interest in this legislation and its impact on Texas physicians.

As the committee knows, physicians regularly handle protected health information; thus our members are acutely aware of the importance of information security. While we certainly support efforts by physicians and others, in general, to protect the privacy and security of sensitive information, we are concerned about the potential unintended consequences of HB 3746 (particularly as applied to physicians and other "covered entities" subject to the Health Insurance Portability and Accountability Act [HIPAA] privacy, security, and breach notification requirements).

HB 3746 would amend Texas' current breach-of-system-security notifications through two amendments. First, it adds a new element to the attorney general notification requirements for breaches involving at least 250 residents of this state. The current law requires notifications to the attorney general to include five elements. HB 3746 would add a sixth element. This would require reporting the number of affected residents who have been sent a disclosure of the breach by mail or other direct method of communication at the time of the notification to the attorney general.

Our concern with this amendment (along with the attorney general breach notification reporting requirement passed last session in House Bill 4390) is that it:

1. **Is inconsistent with the HIPAA notification requirements** to the secretary of the U.S. Department of Health and Human Services (HHS) concerning large breaches. Under HIPAA, larger breaches of 500 or more require reporting to the HHS secretary. Texas' breach of system security requirement has a lower threshold for reporting to the Texas attorney general – 250 residents – and contains elements that vary from the HIPAA requirements;

2. **Creates a complicated and inconsistent dual enforcement framework** for physicians and other HIPAA-covered entities to navigate, which creates additional compliance challenges for these already highly-regulated individuals. The Texas breach notification requirements may be appropriate for those not subject to HIPAA, but they are less so for physicians and other

HIPAA-covered entities, who already are subject to significant breach notification requirements and penalties under federal law and rules after the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009; and

3. **May present an inaccurate picture to the attorney general** when considering enforcement actions under Texas law. We are concerned the attorney general may use this amendment to determine which cases to pursue against persons who report breaches of system security (as Texas law contains fines for each individual for whom notification is due for each consecutive day the reporting person fails to take reasonable action to comply with the subsection). *See* Tex. Bus & Comm. Code §521.151(a-1). Requiring the reporting of the actual number reported at the time of the breach will discourage early reporting to the attorney general (in order to notify the most affected individuals possible before providing the report to the attorney general) and does not sufficiently recognize there are valid reasons under the law why all affected individuals may not have been notified as of the date of reporting to the attorney general, e.g., the law enforcement delay exception under §521.053(d) or the exception under §521.053(b) as needed to determine the scope of the breach and restore the reasonable integrity of the data system.

Next, HB 3746 amends current Texas law to require website posting by the attorney general of larger breaches. The amendment requires a comprehensive listing of the notifications received by the attorney general under §521.151(i), excluding any sensitive personal information that may have been reported to the attorney general under that subsection and any other information reported to the attorney general that is made confidential under the law. The listing must be updated not later than the 30th day after the date the attorney general receives notification of a new breach of system security.

Our concerns with this language are as follows:

- It is duplicative and may be overly punitive as applied to physicians and other covered entities under HIPAA who are already subject to large breach postings by the HHS secretary under the HITECH ACT. *See* Section 13402(e)(4) of the HITECH Act. To inform the public of a breach, notices are not necessary on two separate websites for HIPAA-covered entities (which are also already subject to notification requirements to individuals, the media, and the HHS secretary for larger breaches).

- The bill's website posting requires a "comprehensive" listing of the notifications received by the attorney general, which we are concerned may include information that is sensitive (although "sensitive personal information" itself and confidential-by-law information is removed). Information in the notifications received by the attorney general includes:

    - A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach,
    - The number of residents of this state affected by the breach at the time of the notification,
    - The measures taken by the person regarding the breach,
    - Any measures the person intends to take regarding the breach after the notification under the subsection, and

- Information regarding whether law enforcement is engaged in the breach.

- One of the issues with publicly posting the above-referenced information is that the reporting entity may not have implemented all the mitigation measures listed in the attorney general reporting notification (and its system may still be vulnerable) at the time of the attorney general website posting (which is required to be updated no later than the 30th days after the attorney general receives notification of a new breach of system security). Additionally, the reporting entity may include detailed information in its notification to the attorney general of remedial measures (making it easier for hackers to target the new safeguards they put into place if posted by the attorney general). Consequently, there is a potential that the posting could further compromise data and be used to target practices. This would act at cross purposes with the intent of the law.

  On HIPAA's large breach website postings for cases currently under investigation, the HHS secretary posts very limited information. Even for resolved investigations, the information posted is very limited. This helps prevent the inappropriate use of the information posted by hackers and others who may target reporting entities. The HITECH Act requirement, i.e., Section 13402(e)(4), for posting simply states, "The Secretary shall make available to the public on the Internet website on the website of the Department of Health and Human Services a list that identifies each covered entity involved in a breach described in subsection (a) in which the unsecured protected health information of more than 500 individuals is acquired or disclosed."

- The bill does not include a time after which the required website posting will be removed from the attorney general's website. One of the continuing concerns expressed by HIPAA-entities regarding the HHS secretary's large breach website posting is that the information stays on the website indefinitely. Older, resolved breaches are included in the archives portion of the posting. The information should be removed from the attorney general's website posting entirely after one year if an entity does not have another reportable breach in that period. To post the information indefinitely is overly punitive to individuals who have taken good faith, corrective actions to improve the security of their systems and who may have had their systems hacked despite having reasonable measures in place at the time.

While we think the underlying goal of the bill (i.e., to enhance Texas' enforcement framework for breaches of system security) is laudable as applied to non-HIPAA covered entities, we reiterate that we are concerned about the potential unintended consequences of the legislation, particularly with regard to physicians and other HIPAA-covered entities.

We do not believe that physicians and others who are already regulated as "covered entities" under HIPAA should be subject to Texas' breach-of-system-security notification requirements (as they are duplicative and inconsistent with federal breach notification requirements and subject physicians and HIPAA-covered entities to multiple steep penalty structures at both the state and federal level).

We look forward to continuing to work with you on HB 3746 to address our concerns, and we thank you for your time and consideration. If you have any questions, please do not hesitate to

contact Troy Alexander, director of public affairs, TMA, by email at troy.alexander@texmed.org or by phone at (512) 370-1360.