SUBJECT: Privacy regulations for patient health information

COMMITTEE: Public Health — committee substitute recommended

VOTE: 7 ayes — Kolkhorst, Alvarado, S. Davis, V. Gonzales, Laubenberg, Schwertner, Truitt

0 nays

4 absent — Naishtat, Coleman, S. King, Zerwas

WITNESSES: For — Deborah Peel, Patient Privacy Rights; (*Registered, but did not testify:* Nora Belcher, Texas e-Health Alliance; John Kroll, Gemalto, Inc.)

Against — (*Registered, but did not testify:* Douglas Aycock, National Association of Insurance and Financial Advisors Texas; Brenda Natlon, American Council of Life Insurers; Des Taylor, National Association Insurance and Financial Advisors of Texas)

On — Archie Alexander; Harry Holmes, Harris County Healthcare Alliance; Carolynn Jones, Texas Hospital Association; Thomas Kowalski, Texas Healthcare and Bioscience Institute; Charles Bruce Malone, Texas Medical Association; Stephen Palmer, Texas Health & Human Services Commission; Brad Shields, Texas Federation of Drug Stores; (*Registered, but did not testify:* Paul Carmona, Becky Casares, Office of the Attorney General; Tony Gilman, Texas Health Services Authority; Marjorie Powell, Pharmaceutical Research & Manufacturers of America; Nelson Salinas, Texas Association of Business; Emily Somerville, Genentech, Inc.)

DIGEST: CSHB 300 would prohibit certain persons who collect health information, commonly referred to as covered entities, from selling an individual's protected health information unless it was for the purpose of treatment, payment, or health care operations or was otherwise authorized or required by state or federal law.

Electronic disclosure of protected health information. The bill would require a covered entity to notify individuals before protected health information could be disclosed electronically. This notification could be distributed by posting a written notice at the covered entity's place of

business, on its website, or any other place where the patients involved in the electronic disclosure would be likely to see the notice.

A covered entity also would be prohibited from electronically disclosing an individual's protected health information without obtaining informed consent for each disclosure from a patient or the patient's legally authorized representative. An individual could authorize a disclosure in written or electronic form or orally if documented in writing by the covered entity. Exceptions would be allowed for the purpose of treatment, payment, or health care operations, or if otherwise authorized or required by state or federal law.

The bill would require the attorney general to adopt a standard authorization form in compliance with the Health Insurance Portability and Accountability Act (HIPAA) by January 1, 2013.

Establishing privacy standards. The Texas Health Services Authority (THSA) would be required to develop and submit privacy and security standards for HHSC to review and approve by January 1, 2013. The standards adopted by HHSC would have to comply with HIPAA as well as any other state and federal law relating to the security and confidentiality of health care information that could be electronically maintained or disclosed by a covered entity.

The adopted standards would have to ensure the secure maintenance of identifiable health information and include strategies and procedures on how to disclose the information without violating privacy standards. These rules also would need to support system interoperability with health record databases. THSA would have to establish a process for certification based on a covered entity's past compliance with these standards. THSA would have to publish the adopted privacy rules on its website.

Audits and complaints procedures. HHSC, in coordination with the attorney general, THSA, and the Texas Department of Insurance could request an audit of a covered entity in Texas by the U.S. secretary of health and human services to determine whether or not the entity was complying with HIPAA. These state agencies would have to periodically monitor and review the results of the audits. HHSC also could require a covered entity to audit itself and submit a report with the results.

HHSC would have to review complaints regarding possible unauthorized disclosures of an individual's protected health information and refer the complaint to the appropriate licensing agency or the attorney general, as applicable.

HHSC would have to submit an annual report to the appropriate legislative committees to be published on HHSC's and THSA's websites. The annual report would have to include:

- the number and types of complaints received;
- the enforcement action taken by the HHSC, a licensing agency, or attorney general; and
- the number of audits conducted.

Civil penalties. A court could issue a civil penalty of up to $1.5 million annually against a covered entity found to have established a pattern of repeated violations of disclosing protected health information without authorization. To determine an appropriate penalty, the court would have to assess:

- the seriousness of the violation, including the nature, circumstances, extent, and gravity of the disclosure;
- the covered entity's history of compliance with the law;
- the potential risk of financial, reputational, or other harm to the patient;
- whether the covered entity was certified at the time of the violation;
- the amount necessary to deter a future violation; and
- the covered entity's efforts to correct the violation.

If notified by the licensing agency, the attorney general could pursue an action against a licensed covered entity for a civil penalty and could retain a reasonable portion of the civil penalty to enforce the bill's provisions.

Administrative penalties. CSHB 300 would authorize the executive commissioner of HHSC to impose an administrative penalty on a covered entity that was not licensed by the state and committed a violation, not exceeding $3,000 for each violation. The commissioner would be required to base the penalty amount on the same criteria used to impose civil penalties under the bill.

A covered entity could stop the enforcement of the penalty while the order was under judicial review if it paid the penalty or filed a supersedeas bond with the court in full. If the covered entity could not afford to pay the penalty or file the bond, it could also stop the enforcement by filing an affidavit stating this. The executive commissioner would still be authorized to contest the affidavit, and the attorney general could sue to collect the penalty. A proceeding to impose the penalty would be a contested case under the administrative procedures outlined in Government Code, sec. 2001.

State management of protected health information. HHSC, in consultation with THSA and the Texas Medical Board (TMB), would have to review issues regarding the security and accessibility of protected health information that was maintained by an unsustainable covered entity, meaning one that had ceased to operate. HHSC would submit recommendations to the appropriate legislative committees to:

- determine which state agency should store the protected health information that was recovered by the unsustainable covered entity;
- ensure that the security of protected health information was maintained, including secure transfer methods of this information to the state;
- establish the method and period of time that the state should maintain protected health information;
- establish methods and processes by which an individual would be able to access protected health information after transfer to the state; and
- identify funding for the storage of this information.

HHSC would have to submit the recommendations by December 1, 2012, and this provision would expire January 1, 2013.

Health information technology taskforce. The bill would create a Taskforce on Health Information Technology composed of 11 members that would need to be appointed by the attorney general by December 1, 2012. The composition of the taskforce would be based on the recommendations of the legislative committee chairs. The taskforce chair would be required to have expertise in state and federal health information privacy law, patient rights, and electronic signatures and other consent tools. The positions on the taskforce would be filled by:

- at least two physicians;
- at least two individuals representing hospitals;
- the executive commissioner of the HHSC or a designated employee;
- the commissioner of the Department of State Health Services or a designated employee; and
- the presiding officer of the THSA or a designated employee.

The taskforce would develop recommendations to:

- improve informed consent protocols for the electronic exchange of protected health information;
- improve patient access to electronic health files for personal health; and
- address any other critical issues related to the exchange of protected health information.

The taskforce would be required to submit a report by January 1, 2014 that included its recommendations. The report would have to be published on the THSA website. The taskforce would expire February 1, 2014.

Funding. The bill would require HHSC and the Texas Department of Insurance in consultation with THSA to apply for and actively pursue federal funding to enforce the bill's provisions.

Effective date. The bill would take effect September 1, 2012, and apply to an electronic disclosure of protected health information made on or after the effective date.

SUPPORTERS SAY:

CSHB 300 would protect Texans against the sale or unauthorized disclosure of their personal health information. Patients have expressed many concerns regarding the unauthorized sharing or sale of their private health data. This bill would address these concerns as it would place tight restrictions on how patient data could be shared and would require informed consent by an individual before a provider or other interested party could sell or transfer patient data.

The bill also would establish a framework to investigate complaints for unauthorized uses of patient data and strengthen the civil and administrative penalties issued to known violators. This would create a

major disincentive for covered entities to engage in the sale of patient data and help to remove repeat violators from the health care system.

Our health care system is built upon the trust between a patient and a provider. A person's health outcome is largely dependent upon the individual sharing personal medical history, which could include disclosing sensitive information such as sexually transmitted diseases, mental illness, or domestic abuse. If this type of information is leaked and de-identified, it could impact the patient's ability to purchase health insurance, the cost of coverage, or worse. It could also have a damaging effect on the individual's relationship with health care providers and affect health outcomes.

OPPONENTS SAY:

CSHB 300 would create overwhelming obstacles related to the transfer of health information, which could result in the loss of patient data if a health care provider went out of businesses or merged with another company. Under these circumstances, a provider would be required to get informed consent before transferring a patient's data. Tracking each patient or the legal representative could present challenges in providing high-quality care when it is most needed. Furthermore, a health provider deemed unsustainable would be required to transfer patient records to the state instead of a new health care provider. The state would not be in the best position to ensure continuity of care, and this provision could damage health outcomes by limiting access to historical patient information.

The penalties that could be issued could limit the ability of providers, particularly smaller health care providers like physician's offices or family drug stores, to operate. While it is important to protect patients' privacy, it is unrealistic to assume that every health care provider has the capacity to maintain information in the most sophisticated way. Unintended breaches in even the most secure databases have been known to occur, but the civil penalties outlined under CSHB 300 could be enough to force some providers out of the market, damaging the fragile health care infrastructure in Texas.

OTHER OPPONENTS SAY:

CSHB 300 would represent a huge step forward in protecting patient privacy, but the bill as currently written could do more to prevent unauthorized sharing or sales of a patient's personal health information. Penalties issued to violators should be tougher.

The bill would authorize HHSC to establish privacy protections consistent with HIPAA. However, the federal law on patient privacy is not strong enough. Texas has the opportunity to lead the nation on this issue by enacting stronger protections of patient privacy.

NOTES:

The fiscal note estimates that no significant fiscal impact to the state is expected, but the bill could result in increased revenue from penalties or increased costs resulting from enforcement.