SUBJECT: Protecting the privacy of medical records, providing penalties

COMMITTEE: Public Health — committee substitute recommended

VOTE: 9 ayes — Gray, Coleman, Capelo, Delisi, Glaze, Longoria, Maxey, Uresti, Wohlgemuth

0 nays

SENATE VOTE: On final passage, March 21 — voice vote

WITNESSES: For — Will D. Davis, Texas Association of Life and Health Insurers; Carole Gates, Cigna Corp.; Eric Glenn, Humana, Inc.; John Heasley, Texas Bankers Association; Bruce McAnally; Lisa McGiffert, Consumers Union; Karen Reagan, Texas Retailers Association and Texas Federation of Drug Stores; Kelly Rodgers, Alliance for Responsible Information Practices; Susan Speight, Texas Association of Marriage and Family Planning; Marybeth Stevens, American Council of Life Insurers; *Registered but did not testify:* Allan Chernov, M.D., Aetna; Holli Hill, Health Insurance Association of America; Shirley H. Hutzler, Texas Association of Health Underwriters; Jill M. Ireland; Lee Manross, Texas Association of Health Underwriters; Kim McPherson, The Mental Health Association in Texas; Amy Mizcles, National Alliance for the Mentally Ill of Texas; Karen Neeley, Independent Bankers Association of Texas; Becky Parker; Tyson Payne, Texas Association of Insurance and Financial Advisors; Mike Pollard, Texas Association of Life and Health Insurers; Leah Rummel, Texas Association of Health Plans; Jay Thompson, AFACT, TALHI, Farm Bureau Insurance Co.; Joe Woods, Alliance of American Insurers

Against — None

On — John Blakey, Covenant Health System; Patrick Donoho, Pharmaceutical Care Management Association; Bill Hammond, Texas Association of Business and Chambers of Commerce; Kristin Jenkins, JPS Health Network and Tarrant County Hospital District; Todd Kaufman, Genetech; Alan Mertz, Healthcare Leadership Council; David Pinkus, Small Business United of Texas; Anna F. Stewart; Susan Stone, Texas Children's

Hospital; Matthew T. Wall, Texas Hospital Association; *Registered but did not testify:* Dr. James Guckian, University of Texas System; Beth Mitchell, Advocacy, Inc.; Linda Wiegman, Texas Department of Health

BACKGROUND:

During the interim, the House State Affairs Committee requested the attorney general to prepare a compilation of current Texas laws and regulations that address privacy issues. Also during the interim, the lieutenant governor directed the Senate Health and Human Services Committee to review patient-specific medical information, including prescription data and current statutory and regulatory provisions that govern availability of such information.

On a federal level, the Health Insurance Portability and Accountability Act and Privacy Standards (HIPAA) of 1996, relating to medical records and access to protected health information, specified that if Congress failed to enact a comprehensive health privacy law by August 21, 1999, the secretary of health and human services would have to issue privacy regulations. As a final directive of the Clinton Administration, the privacy rules were due to take effect February 26. However, the Bush Administration decided to delay the effective date until April 14 to allow more time to review the regulations. With that review and approval date, health care providers will not have to comply with the changes fully until April 14, 2003, at the earliest.

In addition to HIPAA standards, the Gramm-Leach-Bliley Act (GLBA), enacted in November 1999, required states, in part, to adopt provisions on privacy and disclosure of nonpublic, personal information, particularly with regard to insurers and financial institutions. The National Association of Insurance Commissioners (NAIC) has developed a privacy model in an effort to assist states in adopting privacy requirements consistent with federal law.

DIGEST:

CSSB 11 would amend the Health and Safety Code to require certain persons who collect protected health information such as medical records to comply with federal HIPAA privacy standards. Further, the bill would amend the Insurance Code to provide that a person who held or was required to hold an insurance license or certificate of authority would have to obtain an authorization to disclose any nonpublic personal health information. The bill also contains enforcement provisions, including civil penalties.

Access to and Use of Health Care Information. *Compliance with federal regulations.* A covered entity would have to comply with HIPAA relating to an individual's access to protected health information, amendment of protected health information, uses and disclosures of protected health information, and notice of privacy practices. To the extent that this legislation would differ from HIPAA, the provisions of the bill would control if they were more restrictive than the provisions of HIPAA.

Information for research. A covered entity or health care entity could disclose protected health information to a person performing health research only if the person performing the research had obtained individual consent or authorization for use or disclosure of the research information required by federal law; the express written authorization of the individual; or a waiver granted by an institutional review board or privacy board as required under federal law.

Privacy board. The bill would establish provisions for the composition and conduct of a privacy board. Conflict of interest guidelines would be imposed. A privacy board could grant a waiver of the express written authorization for the use of protected health information if the board obtained certain related documentation and assurances. A waiver would have to be signed by the presiding officer of the privacy board or his or her designee. The privacy board would review the proposed research at a convened meeting at which a majority of members were present. The waiver would have to be approved by a majority of the privacy board members present at the meeting, unless the privacy board elected to use an expedited review procedure.

A covered entity or health care entity could disclose protected health information to a person performing health research if that entity obtained from the health researcher certain representations as to the use and necessity of the information. A person who was the subject of protected health information collected or created in the course of a clinical research trial would be able to access the information at the conclusion of the research trial.

Disclosure of information to public health authority. A covered entity could use or disclose protected health information without the express

written authorization of the individual for public health activities or to comply with the requirements of any federal or state health benefit program or any federal or state law. Under the bill, a covered entity could disclose protected health information to certain public health authorities or state agencies.

Prohibited Acts. *Reidentified information.* A person could not reidentify or attempt to reidentify an individual who was the subject of any protected health information without obtaining the individual's consent or authorization if required by state or federal law.

Marketing uses of information. A covered entity would not be able to disclose, use, sell, or coerce an individual into consenting to the disclosure, use, or sale of protected health information, including prescription patterns, for marketing purposes without the consent or authorization of the individual who was the subject of the information. The bill would set forth requirements for written marketing communications.

Enforcement. *Injunctive relief, civil penalties.* The attorney general (AG) could institute an action for injunctive relief to restrain a violation, as well as an action for civil penalties against a covered entity or health care entity for a privacy violation. An assessed civil penalty could not exceed $3,000 for each violation. If a court found that violations had occurred with such a frequency as to constitute a pattern or practice, the court could assess a civil penalty as high as $250,000.

Disciplinary action. In addition to the above penalties, a violation by an individual or facility that was licensed by a state agency would be subject to investigation and disciplinary proceedings, including probation or suspension by the licensing agency. If there were evidence that the violations constituted a pattern or practice, the agency could revoke the individual’s or facility’s license.

Exclusion from state programs. In addition to the above penalties, a covered entity would be excluded from participating in any state-funded health care program if there were evidence that the covered entity engaged in a pattern of practice that violated the bill’s provisions.

Other remedies. This bill would not affect a person's right under other law to bring a cause of action or otherwise seek relief with respect to conduct that was in violation of these provisions.

General provisions. *Applicability.* CSSB 11 would not affect the validity of another state statute that provided greater confidentiality for information made confidential by this legislation.

Sovereign immunity. The provisions of this bill would not waive sovereign immunity to suit or liability.

Rules and compliance. A state agency that licensed or regulated a covered entity could adopt rules as necessary to carry out the provisions of this legislation. A covered entity would have to comply with the amended provisions of the Health and Safety Code under this bill not later than September 1, 2003.

Exemptions. *Partial exemption.* Except for provisions relating to marketing uses of information, the bill's provisions regarding medical records privacy would not apply to a covered entity as defined in HIPAA, certain entities associated with a covered entity, the holder of an insurance license, an entity established under the Texas Workers' Compensation Insurance Fund.

Transactions by financial institutions. To the extent that a covered entity engaged in the activities of a financial institution, or authorized, processed, cleared, settled, billed, transferred, reconciled, or collected payments for a financial institution, this bill and any rule adopted under it would not apply.

Nonprofit agencies. The Texas Department of Health (TDH) by rule would exempt from privacy provisions a nonprofit agency that paid for health care services or prescription drugs for an indigent person only if the agency's primary business was not the provision of health care or reimbursement for health care services.

Other exemptions. Provisions relating to medical records privacy would not apply to worker's compensation insurance, functions, or related entities; an employee benefit plan and related entities; certain state agencies responsible

for special needs offenders; and certain educational records covered by other federal acts. Also, the provisions would not prohibit the American Red Cross from accessing any information necessary to perform its duties related to disaster relief or emergency leave verification services for military personnel.

Privacy of health information. *Privacy notice and disclosure authorization.* CSSB 11 would amend the Insurance Code to provide that a person who held or was required to hold an insurance license registration, certificate of authority, or other authority ("licensee") would have to obtain an authorization to disclose any nonpublic personal health information before doing so. The bill would establish requirements for a written or electronic request for authorization. The right of a consumer or customer to revoke an authorization at any time would be subject to the rights of an individual who acted in reliance on the authorization before receiving notice of a revocation.

Delivery of authorization. A request for authorization and an authorization form could be delivered to a consumer or a customer if the request and form were clear and conspicuous.

Exceptions. A licensee could disclose nonpublic personal health information to the extent that the disclosure was necessary to perform certain specified insurance functions on behalf of the licensee, including, but not limited to: underwriting, loss control services, ratemaking and guaranty fund functions, risk management, utilization review, peer review activities, case management, disease management, and actuarial, scientific, medical, or public policy research.

Exception for compliance with federal rules. These provisions would not apply to a licensee who was required to comply with federal standards governing the privacy of individually identifiable health information.

Protection of Fair Credit Reporting Acts. This bill could not be construed to modify, limit, or supersede the federal Fair Credit Reporting Act. Further, the bill would not preempt or supersede a state law related to medical record, health, or insurance information privacy that is in effect on July 1, 2002.

Violation, penalties. The Texas Department of Insurance (TDI) could investigate any alleged violation by a licensee of provisions related to privacy of health information and could impose fines and other sanctions as determined to be appropriate.

Rules and compliance. The commissioner could adopt rules to implement provisions related to this legislation. The compliance date could be delayed if the commissioner determined that an entity needed more time to establish policies and systems in order to comply with the bill's requirements.

Changes made by this bill to the Health and Safety Code would take effect on September 1, 2001, and to the Insurance Code on January 1, 2002. An authorization or consent granting access to an individual's health care records executed before the effective dates of this bill would be governed by the law in effect when the authorization or consent was executed.

SUPPORTERS SAY:

CSSB 11 would establish provisions relating to privacy of medical records and nonpublic health information that now are accessed, analyzed, and distributed by a large number of third parties, including health care providers, clinical researchers, and insurers. Much of the language of this bill would track federal standards under HIPAA and would allow for even stronger protections in areas such as marketing.

A downside of the Information Age is the sharing of data considered by many to be private. An individual's medical condition and treatment, including drugs prescribed by a physician, should remain confidential, yet companies compile and frequently distribute such information for marketing and other purposes. That a company can randomly obtain information considered confidential between a patient and his or her doctor and pharmacist is a personal intrusion. Information this sensitive could be abused in ways detrimental to an individual, such as denying a job to someone who had a specific illness but who might be able to do the work, regardless of a particular medical condition. A worst-case scenario would be someone who might not seek medical treatment for fear of having sensitive information released to a third party without the individual's consent or someone who was not truthful or straightforward about medical information for fear of repercussions unrelated to medical treatment.

This bill would offer protection from invasions related to medical and other private information. It would state that a covered entity could not disclose or use an individual's protected information, including prescription patterns, for marketing purposes without the consent or authorization of the individual. In other words, the patient would have to give the third party permission to obtain such personal information for marketing. This legislation would treat violations of these provisions seriously and would allow the AG to obtain injunctive relief and civil penalties of $3,000 for each violation. If a court found that there was evidence of a pattern of violations, the fine could reach as high as $250,000, an intended deterrent for unscrupulous violators.

In addition, this legislation would exceed protections offered by HIPAA, which extend only to a health care provider, a health care plan, or a health care clearing house. This bill would extend the definition of a covered entity to include a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, or person who maintained an Internet site, including an employee, agent, or contractor of all such entities.

It's time the Legislature acted to protect individuals' medical records and other personal information from being used unknowingly or unwittingly, and this bill is a significant step.

OPPONENTS SAY:

This bill would be a tiny step in the scheme of privacy protection that only would fill in a few gaps resulting from HIPAA. Despite the fact that a third of the bill applies to the Insurance Code, CSSB 11 would exempt almost all activities of insurers or "licensees." For example, a licensee could disclose nonpublic personal health information to the extent necessary to perform functions, including underwriting, loss control services, ratemaking and guaranty fund functions, risk management, utilization review, peer review, and actuarial, scientific, medical, or public policy research. The exception for actuarial, scientific, medical, or public policy research alone is excessively broad and could be a means for permitted or allowable disclosure of nonpublic information that would violate an individual's privacy without any recourse.

Although the AG could seek injunctive relief and penalties for violations under this legislation, the bill would not go far enough in protecting

individuals. Violations of a person's privacy are serious and warrant a private cause of action. An individual should be able to bring suit under this bill and to seek appropriate relief, such as through the Deceptive Trade Practices Act.

NOTES:

The committee substitute added to the Senate engrossed version a provision that would not affect the validity of another statute that offered greater confidentiality. Also, the substitute would exempt from the legislation workers' compensation insurance or functions and financial institutions, to the extent that their activities included processing payment transactions. The substitute also would grant the insurance commissioner rulemaking authority.