LEGALLY SPEAKING

A New Item to Watch in 2008

U.S. Senate Bill 1814, the Health Information Privacy and Security Act (HIPSA)

By Terrell J. Isselhard, Esq.

What could possibly come in the wake of HIPAA? Alas, another H acronym. The Health Information Privacy and Security Act (HIPSA) represents the very real possibility of another legislative layer to your practice of medicine. Covered entities (anyone currently handling health information) need to keep a wary eye on SB 1814, currently under consideration by the Committee on Health, Education, Labor, and Pensions. HIPSA could change the current HIPAA landscape in several ways.

First, the bill would obligate the Secretary of the Department of Health and Human Services (HHS) to revise the HIPAA Privacy and Security Rules to conform with HIPSA's requirements. Second, an "opt-out" provision would require health care entities to permit their patients to choose to have their protected health information (PHI) excluded from the entity's electronic systems. Third, the bill imposes both criminal and civil sanctions on those who violate the privacy rules. And, finally, there are Security Rule additions.

The opt-out issue. Some attorneys and administrators fear that these provisions would require health care entities to give patients the choice of refusing to have their health information maintained in electronic formats. As more health care entities transition to electronic medical records (EMRs), the prospect of patients' selective exclusion from EMRs poses a significant threat to complete reliance on EMRs.

Patients would decide

Under the proposed HIPSA provisions, patients would decide whether to be included in an EMR. This would require that the entity "not access, maintain, retain, modify, store, destroy or otherwise use or disclose an individual's protected health information *for other than treatment or payment purposes* until that patient has been given an opportunity to opt out of that disclosure." The entity must provide individuals with a simple description of the information systems used to transmit or disclose PHI, and a statement of the individual's right to opt out of the entity's health information network or system. The individual must be given adequate time to exercise that option and instruction on how to do so. Furthermore, the authorization to disclose must include a description of the nature and probability of harm to the individual resulting from authorization for use of disclosure. (A summary of SB 1814 is available at http://leahy.senate.gov/press/200707/071807c.html.)

Loophole found in bill

In its current form, HIPSA would not completely preclude hospitals from transitioning to electronic health records. The loophole for their continued use is found in Section 104(d) of the bill stating that an entity may not access, maintain, or otherwise use or disclose PHIs *for other than treatment or payment purposes*. This is the only exception and it essentially creates an opt-out provision. Further, if hospitals want to disclose PHIs to third parties in order to continue treatment (e.g., send the records to a different health care provider) or ensure payment (e.g., transmit information to a collection agency), patients would not be able to opt out of such disclosure. At this time it remains unclear how the HHS may interpret the other opt-out sections, including the phrase, "for other than treatment or payment purposes." The manner in which the HHS interprets this phrase could significantly affect the information contained in the databases.

Why additional criminal and civil sanctions and why now? The perceived lackluster enforcement of HIPAA rules caused a backlash that spawned a new pro-active movement away from complaint-

based voluntary compliance and toward direct cross-agency audits and new legislation to increase HIPAA privacy and security enforcement.

SB 1814, introduced by Senators Edward Kennedy and Patrick Leahy, does not seek to supplant HIPAA, but requires the HHS to revise HIPAA to be consistent with HIPSA. HIPSA requires the establishment of an Office of Health Information Privacy at HHS and gives it enforcement power to impose criminal and civil penalties. It also directs the attorney general to "debar" health entities from receiving federal programs if found guilty of wrongful disclosure of PHI. Another large addition is that HIPSA would permit individuals to sue for compensatory damages and receive punitive damages in cases of unauthorized disclosure.

Moreover, HIPSA would authorize state attorney generals to sue on behalf of residents and protect whistle blowers who report violations from retaliation. As proposed, HHS would delegate to the director of the Office for Civil Rights (the agency within HHS that enforces the HIPAA Privacy Rule) the authority to issue subpoenas in investigations of alleged violations.

No fines yet imposed

Note: in the four-plus years since the April 14, 2003, compliance deadline, the Office for Civil Rights reports that no fines have been imposed. Approximately 29,994 complaints were received between 2003-2007 and of them, 23,734 or about 79%, have been closed and resolved, while 21% remain open. Of complaints that were investigated, approximately 67% obtained corrective action; no violation was found in about 33%.

The Security Rule. While HIPSA requires the DHHS, via the establishment of an Office of Health Information Privacy, to enforce HIPSA, the Security Rule mandates authority to the Centers for Medicare & Medicaid Services (CMS) to enforce the Security Rule on any covered entity that creates, maintains or transmits electronically.

While CMS has not investigated any providers (as of November 2007) for compliance with the Security Rule since its April 20, 2005, compliance deadline, the Office of the Inspector General, HHS, and the Government Accountability Office have increased enforcement measures, particularly those relating to remote use of electronic PHI.

The recent number of high-profile security incidents, and the media reports that followed, spurred the CMS to publish "HIPAA Security Guidance for Remote Use of Access to Electronic Protected Health Information." This guidance specifically addresses the use of portable medical devices and off-site access and transmission of electronic PHI.

The publication specifically notes that CMS has the authority to enforce the Security Rule with the Office for Civil Rights having enforcement authority over the Privacy Rule. In addition, the OIG conducted an audit of Atlanta's Piedmont HealthCare, Inc., in March 2007—the first hospital provider to undergo such an audit. According to the OIG Work Plan for 2007, it will "review" CMS' experience implementing HIPAA regulations for the Medicare and Medicaid programs to "identify key issues" for HHS' health information technology initiative.

New right for patients?

In conclusion: If signed into law, HIPSA, as currently drafted, would add new urgency to the enforcement of health information privacy and would dramatically alter the environment of prosecution. The statute would also create a new right for patients to file a lawsuit for breach of privacy and security violations. While tough civil monetary penalties and other sanctions have not yet been imposed under HIPAA, HIPSA could provide a powerful punch (as opposed to slaps) within the health-care arena. The introduction of SB 1814 is a small beginning—but a sign that agencies are getting serious about pro-active enforcement. ■

The author is an equity partner in the Chicago-based health law firm of Chuhak & Tecson, PC. Comments and suggestions should be e-mailed to Mr. Isselhard at tisselhard@chuhak.com.