Statement
of the
Confidentiality Coalition
to the
Senate Commerce, Science and Technology Committee
Consumer Protection, Product Safety, and Insurance Subcommittee

Data Security and Breach Notification Act of 2010

September 22, 2010

The Confidentiality Coalition thanks the Senate Commerce, Science and Technology Committee for the opportunity to submit a statement for the record on the "Data Security and Breach Notification Act of 2010" (S.3742). The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health produce distributors, pharmacy benefit managers, pharmacies, health information and research organizations, patient groups, and others[1] founded to advance effective patient confidentiality protections.

The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions. The Confidentiality Coalition is committed to ensuring that consumers and thought leaders are aware of the privacy protections that are currently in place. And, as healthcare providers make the transition to a nationwide, interoperable system of electronic health information, the Confidentiality Coalition members believe it is essential to replace the current mosaic of sometimes conflicting state privacy laws, rules, and guidelines with a strong, comprehensive national confidentiality standard.

As such, the Confidentiality Coalition believes that the privacy of patients' health information is of the utmost importance. Nothing is more important to engendering trust in the healthcare system than a comprehensive set of privacy protections for personal health information. That said, we have concerns that S. 3742 would result in health information being governed needlessly by two entities – the Federal Trade Commission (FTC) under the current Senate bill and the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA).

[1] A list of the Confidentiality Coalition members is attached to this letter.

The Data Security and Breach Notification Act of 2010 would require the Federal Trade Commission (FTC) to establish regulations requiring a broad range of entities, including healthcare organizations, to implement security practices to protect personal information and to provide for notification in the event of any security breaches of that information. The protections proposed by S. 3742 unnecessarily duplicate the protections already in place under HIPAA, and would likely have disruptive effects on the normal business activities of healthcare organizations by altering current and accepted practices across the industry. In other words, the legislation would create a parallel and inconsistent enforcement mechanism for the healthcare industry, which is already subject to comprehensive and effective privacy and security regulation at both the federal and state levels.

Accordingly, we encourage a clear statement in this legislation that exempts healthcare companies that are HIPAA "covered entities"[2] and their "business associates"[3] from the reach of this new legislation. This clarification would preserve the careful lines drawn by the HIPAA privacy and security rules and would permit the healthcare industry to continue to provide services to members and patients without the need to dramatically alter its current (and already heavily regulated) arrangements. We view this exemption as appropriate to avoid substantial disruption of the important work conducted by healthcare organizations on behalf of patients and consumers.

Discussion

The Confidentiality Coalition applauds Congress' effort to require entities holding sensitive consumer information to develop a comprehensive data compliance protection plan and adhere to strict breach reporting requirements. While we understand and support these goals in connection with currently unregulated arenas, these goals - and the consumer risks they are designed to address - have already been addressed for the healthcare industry. The healthcare industry is heavily regulated in its privacy and security obligations. These obligations have been in place since 2003 under HIPAA, and recently have been revised and expanded through the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act (P.L. 111-5).

---

[2] 45 CFR 160.103 Covered entity means: (1) A health plan; (2) A health care clearinghouse; (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

[3] 45 CFR 160.103 Business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity.

The HIPAA privacy and security rules apply to "protected health information" – health information that is held by a HIPAA covered entity. It is information that either directly identifies an individual or for which there is a reasonable basis to believe that an individual could be identified. Protected health information includes demographic information, such as a person's name and address. It includes payment information – such as credit card information or checking account information – that a patient uses to pay for care. Generally, all identifiable information about a patient that is held by a HIPAA covered entity is protected health information and, therefore, governed by HIPAA.

The HIPAA regulations include a number of components – most importantly, baseline privacy regulations as well as security regulations that apply specifically to electronic information. These HIPAA/HITECH provisions impose specific requirements on covered entities to provide notice to patients and members of all uses and disclosures of personal information obtained in the course of providing services to these individuals. In addition to the detailed privacy notice, the HIPAA/HITECH rules impose specific consent obligations, with certain areas where consent is assumed (primarily, the core healthcare purposes of treatment, payment, and healthcare operations), certain areas where use and disclosure is permitted without the need for consent (such as certain public health disclosures or disclosures in connection with litigation), and other areas – essentially, all other disclosures – where a specific, detailed individual "authorization" is required.

"Marketing" in connection with the healthcare industry also is heavily regulated and limited – both through the original HIPAA rules and through new, stricter, provisions in the HITECH Act. These rules address the specific operations of healthcare companies and under these rules, most marketing activities require a specific patient authorization. The only marketing activities that are permitted without authorization are those that the Department of Health and Human Services (HHS) has deemed to be useful and appropriate for consumers in the healthcare industry. The HHS Office of Civil Rights has jurisdiction to enforce these provisions (including expanded new penalties created by the HITECH Act). In addition, the HITECH Act authorizes state Attorneys General to enforce the HIPAA rules.

As evidenced above, the HIPAA privacy and security rules provide a comprehensive privacy and security framework for HIPAA covered entities. Initially, "business associates" under HIPAA – those companies that provide services to HIPAA covered entities – were regulated through contracts with these covered entities. Now, as a result of the HITECH law, these business associates also are directly subject to privacy and security requirements, subject to primary enforcement by HHS, and face the same penalties as covered entities for non-compliance. Thus, all organizations handling protected health information are subject to the same stringent requirements and penalties for violations or breaches of this information.

Accordingly, while HIPAA does not apply to all entities that might collect, use, or disclose health-related information,[4] HIPAA does create a comprehensive set of standards and an overall

[4] The Coalition supports efforts by Congress and the Federal Trade Commission to evaluate appropriate privacy and security obligations for these unregulated healthcare entities or for uses and disclosures of sensitive healthcare information that are outside the scope of HIPAA.

enforcement protocol for those entities – both covered entities and business associates – who are regulated directly under the HIPAA rules. Moreover, as a result of the HITECH law, both covered entities and business associates face significantly increased exposure for violations of these rules, as well as the ongoing possibility of criminal penalties.

Therefore, for these covered entities and business associates, regulation under HIPAA/HITECH is both comprehensive and substantial. HIPAA/HITECH incorporates a wide range of standards for the use and disclosure of health information, creating specific rules for all aspects of the operations of the covered entities and their business associates. Moreover, the HIPAA Security Rule imposes perhaps the most significant set of security–related requirements imposed by law under any standard.

In addition to detailed privacy and security regulations, the HITECH Act includes new rules for responding to security breaches. HIPAA covered entities and their business associates are required to notify each individual whose information is breached. For larger breaches – those involving the health information of 500 or more individuals – these organizations also must notify the media. The Secretary of HHS also must be notified of all breaches, large and small. HHS posts a list of breaches on its web site.

The HIPAA breach regulations include specific requirements for how individuals must be notified. These reflect the requirements Congress established under the HITECH Act. For example, individuals must be notified of a breach without unreasonable delay, and no later than 60 days after the breach is discovered. The notice must be in writing; it must describe the type of information breached and the steps individuals should take to protect themselves from potential harm resulting from the breach. Thus, HIPAA covered entities already are obligated to carry out the kinds of security breach activities that S. 3742 requires.

With these standards in place, we have significant concerns about the risks and burdens of creating unnecessary additional obligations related to breach notices for healthcare entities. S. 3742 would create a new and inconsistent set of obligations on both notice and consent for the healthcare industry. We recognize that there is language addressing entities in "compliance with any other Federal law that requires such covered entity to maintain standards and safeguards for information security and protection of personal information in the legislation (in the section entitled "Treatment of Entities Governed by Other Law"), but the effect of this language as drafted is unclear. Therefore, to the extent that this legislation applies to healthcare entities and their business associates, we believe strongly that these provisions would require fundamental changes in the healthcare industry without any identified need or specific rationale.

The HIPAA rules – particularly with the additional obligations imposed by the HITECH Act – create a challenging set of standards for any affected healthcare entity. To apply different or additional standards to this information would create significant additional cost and unneeded complexity.

Also, there is no need for an additional regulator to oversee these obligations. The Department of Health and Human Services has primary authority under these rules, with a significant new set of enforcement tools in its arsenal. There is no need for FTC to enter this arena to provide additional (and potentially inconsistent) regulatory oversight. To the extent that Congress wants

FTC to have any involvement at all in the regulation of health information, it should limit this involvement (if any) to those entities that are outside the HIPAA/HITECH structure. Congress should not permit the FTC to regulate those companies – whether a covered entity or a business associate – who already face regulation by HHS and the Attorneys General around the country.

Therefore, we encourage Congress to amend S. 3742 by crafting a clear and explicit exemption for personal information held by covered entities and their business associates that is already protected and regulated by HIPAA. Specifically, Congress should ensure that there is an explicit statement in the legislation that entities covered by HIPAA and their business associates are exempt to the extent that the information they hold is protected and regulated by HIPAA. This specific language should recognize that the privacy and security practices of the healthcare industry already are heavily regulated, with principles designed to facilitate the appropriate use and disclosure of healthcare information for appropriate purposes. Any change to these rules in legislation that is focused on the activities of the healthcare industry would be duplicative at best and disruptive and damaging for patients at worst.

We look forward to working with you as this bill moves through the legislative process and hope you can address the concerns we have raised. The Confidentiality Coalition appreciates the opportunity to continue our discussion with you on this legislation. If you have any questions or would like further information, please contact Tina Olson Grande, Sr. Vice President for Policy, at the Healthcare Leadership Council and Executive Director of the Confidentiality Coalition (tgrande@hlc.org).