American Hospital Association

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802
(202) 638-1100 Phone
www.aha.org

Statement

of the

American Hospital Association

to the

Senate Commerce, Science and Technology Committee

Consumer Protection, Product Safety, and Insurance Subcommittee

The Data Security and Breach Notification Act of 2010

September 22, 2010

The American Hospital Association (AHA), on behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our 38,000 individual members, appreciates the opportunity to share its views on the Data Security and Breach Notification Act of 2010. This proposed legislation would require the Federal Trade Commission (FTC) to establish regulations requiring a broad range of entities, including many hospitals, to implement security practices to protect personal information and to provide for notification in the event of any security breaches of that information.

Hospitals already are regulated in this area. In the past, Congress has recognized this by exempting hospitals from duplicate regulatory requirements. We believe that a similar approach makes sense here.

My testimony will focus on the following:

- The scope and requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and how HIPAA protections for patient information recently have been strengthened.
- How the FTC and the Department of Health and Human Services (HHS) currently operate parallel and separate rules for security breaches.
- Why this approach – exempting HIPAA covered entities from the FTC rules – makes sense.

America's hospitals are dedicated to safeguarding the privacy of their patients' medical information. The AHA and its members have supported efforts by the Department of Health and Human Services (HHS) to implement HIPAA. Under HIPAA, HHS has established detailed requirements for how HIPAA covered entities must protect the privacy and security of the patient information they maintain. These include rules for notifying patients in the event of a security breach. Hospitals are deeply familiar with the type of

obligations proposed in this legislation, and indeed already are subject to a very similar regulatory framework.

HIPAA was first enacted in 1996. In 2009, Congress strengthened the HIPAA privacy and security requirements as well as created a federal framework for data breach notification for HIPAA covered entities. Under the HITECH Act – part of the American Recovery and Reinvestment Act of 2009 – HIPAA now contains stronger enforcement mechanisms and higher penalties for noncompliance. State attorneys general now have the power to bring enforcement actions under HIPAA, in addition to HHS. The HITECH Act also gave more rights to patients. Patients now have an even greater ability to control how their information is used and to whom it is disclosed. Perhaps the most significant change under the HITECH Act is that the HIPAA rules now apply not only to HIPAA covered entities, but also directly apply to their subcontractors, known as business associates.

The protections proposed under the Data Security and Breach Notification Act duplicate those already in place under HIPAA. For hospitals and other HIPAA covered entities this Act would require a whole new set of compliance activities that largely mirror HIPAA. This Act may also subject hospitals to two parallel sets of enforcement activities; penalties could apply under each set of requirements. Requiring HIPAA covered entities to establish compliance standards for two different regulatory regimes will cost hospitals money. Because hospitals already must meet HIPAA's stringent data security standards, these additional compliance costs will not afford consumers any greater protection.

Information Protected by HIPAA

The HIPAA privacy and security rules apply to "protected health information." Basically, this is 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, like 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 hospital is protected health information and is governed by HIPAA.

For almost a decade, HIPAA has provided a comprehensive framework for protecting the privacy and security of this patient information. The AHA's members are experienced in taking the steps necessary – and required by HIPAA – to protect patient information. The HIPAA regulations include a number of components – most importantly, baseline privacy regulations as well as security regulations that apply specifically to electronic information. The privacy regulations under HIPAA impose detailed rules about how a hospital may use patient information and when and to whom a hospital may disclose that information to another party.

For example, a hospital is allowed to use all of the information in a patient's medical record to treat a patient. Not all information, however, can be sent to a health plan to obtain payment for that care. The

privacy regulations contain rules for almost every circumstance. There are rules about when a hospital can disclose patient information to a subcontractor – or business associate. There are rules establishing when a hospital must seek special permission from a patient before using that patient's information, such as to conduct research. There are rules for when and how patient information may be disclosed pursuant to a subpoena. And there are rules about how the information on minors and on deceased patients can be used. Hospitals simply do not and cannot do anything with patient information without referring to the HIPAA requirements.

HIPAA also contains security requirements. These are detailed requirements for maintaining the security of electronic information. HIPAA covered entities must put in place safeguards to protect the confidentiality, integrity, and security of electronic protected health information. As with the privacy requirements, these security requirements cover virtually every circumstance under which patient information is stored or transmitted electronically in the hospital setting. For example, a hospital must have a process in place for identifying and assessing reasonably foreseeable vulnerabilities in its information systems. Corrective actions are required to address any vulnerabilities identified.

HIPAA requires its covered entities to take a number of steps to comply with the privacy and security regulations. Hospitals are required to have detailed HIPAA policies and procedures and to train their employees on those practices. They also must appoint a privacy official and a security official responsible for managing the privacy and security practices.

HIPAA Requirements for Security Breaches

In addition to detailed privacy and security regulations, the HIPAA regulations include new rules for responding to security breaches. This is a result of the HITECH Act. A HIPAA covered entity, such as a hospital, is required to notify each individual whose information is breached. For larger breaches – those involving the health information of 500 or more individuals – a hospital also must notify the media. The Secretary of HHS also must be notified of all breaches, big 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. HIPAA covered entities already are obligated to carry out the kinds of security breach activities that this proposed legislation requires.

Separate Rules for HIPAA and Non-HIPAA entities

The HITECH Act established two parallel sets of rules for security breaches. One is under HIPAA, governed by HHS. Another set of rules covers a different kind of information – personal health records. These are records that any one of us can set up on a publicly available web site to store our health information ourselves. They can contain personal, sensitive information. But the information isn't protected by HIPAA, because it is not maintained by a hospital or other HIPAA covered entity. Instead, the information is maintained by the vendor of the web site and by the consumer. For these kinds of records, the Federal Trade Commission has authority to set the rules.

These two sets of security breach rules don't overlap. This is because, in the HITECH Act, Congress recognized that there is an existing privacy framework for HIPAA covered entities. Congress established a separate set of breach requirements under HIPAA and excluded HIPAA covered entities from the new FTC requirements. The AHA believes that this same approach makes sense going forward. Hospitals already follow a strict set of requirements for protecting patient information and for addressing security breaches.

Subjecting HIPAA covered entities and their business associates to the Data Security and Breach Notification Act would require hospitals to establish two parallel compliance programs, set up by two different federal agencies. One to meet the long-standing HIPAA requirements, and another to comply with the FTC regulations that would be developed under this legislation. Inevitably, this will increase a hospital's compliance costs, but without increasing the security of patient information. Hospitals already are responsible for protecting patient information. Increased compliance costs have the effect of increasing health care costs, a result none of us wants.

There also is the potential that hospitals would be subject to two sets of penalties – one from HHS and one from the FTC – for the same security incident. We understand that under the Act the FTC would have the discretion to determine that HIPAA covered entities and their business associates are deemed in compliance with the Act by virtue of their HIPAA obligations. But even if the FTC takes this step, it is possible that, where a HIPAA covered entity failed to comply with HIPAA, it would be subject not only to the new and enhanced HIPAA penalties, but also to the FTC's penalties.

We believe it also is in the best interest of consumers for HIPAA covered entities and their business associates to be expressly exempted from the Act. If a hospital is required to comply with both the FTC and the HHS rules regarding security breaches, the hospital could be required to send two letters to the same patient for the same security incident. That simply doesn't make sense for patients, and it doesn't increase the protection of their information. In order for consumer notice of security breaches to be meaningful, it is important that consumers not receive multiple notices of a single data breach. It will be confusing for individuals to receive multiple letters about the same breach. If there are too many notices, at some point, letters about security breaches will become just more white noise. Consumers may end up disregarding important information and fail to take steps to protect against future harm or misuse of their information. Consumers should receive a single notice for a single breach.

HIPAA covered entities and their business associates are fully and vigorously regulated by HHS. They already are obligated to comply with detailed requirements designed to protect the security of patient information. Where those systems fail, they must notify patients of a security breach, as HHS requires. An additional set of rules will be cumbersome and costly, both for hospitals and for patients.

We appreciate the Subcommittee's interest in these issues and thank you for the opportunity to testify.