TESTIMONY BEFORE THE UNITES STATES SENATE JUDICIARY COMMITTEE
ON
"HEALTH IT: PROTECTING AMERICANS' PRIVACY IN THE DIGITAL AGE"
January 27, 2009
By John P. Houston
Vice President, Information Security and Privacy; Assistant Counsel
University of Pittsburgh Medical Center

I am grateful for the opportunity to address the Senate Judiciary Committee regarding this important topic. I would like to start by stating that the adoption of Healthcare Information Technology (Health IT) is one of the most significant healthcare initiatives that this nation can undertake. The adoption of Health IT will lead to substantial improvements in healthcare delivery, reductions in medical error rates, reductions in costs and improvements in population health, while accelerating medical research. However, the widespread adoption of Health IT will not be successful if our patients' privacy expectations are not met. The reality is that we are all patients at some point in our lives, and as such, we expect that our medical records will remain confidential. This reality drives healthcare professionals to make the appropriate decisions regarding privacy practices.

I am proud to say that UPMC has one of the most progressive and longstanding programs for the development and deployment of health IT in the world. For example:

? UPMC's new Children's Hospital will utilize an entirely electronic medical record, leaving no accommodations for paper medical records.

? UPMC's system currently has over 24,138 users, and 3,075,273 unique electronic patient records.

? Computerized Physician Order Entry (CPOE) is deployed at 46% of UPMC's inpatient units while nationally the rate is less than 2%.

? UPMC's ambulatory electronic medical record (EMR) is deployed to 60% of UPMC's 2,300 employed physicians. The national benchmark is 4%.

? UPMC has invested more than $1 billion in information technology over the last five years to improve the quality, safety and efficiency of patient care.

? Both, UPMC Presbyterian and Children's Hospital of Pittsburgh have achieved Stage 6 of the HIMSS Analytics EMR Adoption model. This level recognizes facilities that have provided their caregivers with advanced EMR functionality that includes: ancillary systems, clinical data repository, decision support, CPOE, Positive Patient Identification and physician documentation within an integrated EMR. The average U. S. hospital is automated to the Stage 2 level.

UPMC's health system features:

? 50,000 employees

? More than $7 billion in revenue

? 20 tertiary, specialty, and community hospitals (including a psychiatric hospital, a children's hospital, and a women's hospital)

? 400 outpatient sites and doctors' offices, with approximately 3 million patient visits per year

? Retirement and long-term care facilities

? An insurance plan that covers 1.3 million members through a variety of insurance programs

Having been accountable for both privacy and information security at UPMC for the last eight years, I believe that
I have developed a deep understanding for both. I am not only aware of the public policy considerations underlying privacy and information security, but also the operational balance between a patient's right to privacy, and providing timely and complete information necessary for the delivery of effective health care. Unfortunately, this balance is neither precise nor clear. I have seen firsthand how information barriers established in the interest of privacy have detrimentally affected patient care.

I have reviewed the current draft of the privacy legislation that was included in the "Health Information Technology for Economic and Clinical Health Act'' (the "Act"). While the Act attempts to address the evolving privacy and security requirements that have arisen since the implementation of HIPAA, it falls short of providing a comprehensive and workable framework. In too many cases, the Act calls for study or review. In other cases, the Act imposes obligations that are overly burdensome, while falling short of advancing privacy. I believe that we would be better served by spending additional time to develop a comprehensive and balanced privacy and security framework, than by adopting these privacy and security rules.

Regarding the privacy and security sections of the Act, I have the following comments:

Business Associates.

I agree that business associates and others should be held to the same privacy and security standard as covered entities. In addition, obligating business associates to notify the covered entity of a breach further strengthens existing HIPAA requirements. However, statutory guidance is necessary regarding enforcement, and to define a

covered entity's responsibilities, with regard to the act of the business associate. Without such guidance, the Act may impede the operation of business associates and covered entities.

Patient Notice of Breaches

Under HIPAA, the covered entity is required to make an accounting of disclosure in any case where an inappropriate disclosure has occurred. While the Act reasonably requires the covered entity to notify a patient of a breach of the patient's health information, in certain cases it also requires the covered entity to post breaches on its website. In other instances, the Act requires the covered entity to notify the media. Additionally, the Act calls for the reporting of all breaches to HHS.

I am concerned that there will be limited practical benefit associated with the website posting or media notice, in relation to the associated effort. Further, it would appear that the purpose of reporting breaches is punitive, rather than serving a constructive purpose.

Technology Standards.

The Act provides that technologies shall be specified for securing identifiable health information. While the concept of establishing specific standards may seem appealing, technologies and security threats change on an almost daily basis. Furthermore, requirements vary greatly between covered entities, based on how they have implemented technology. Therefore, the establishment of specific standards may actually retard or prevent the adoption of appropriate security measures.

Restrictions on Certain Disclosures of Health Information.

The act provides that patients have the right to restrict a health plan from gaining access to aspects of their record, related to privately paid patient services. In practice, such restrictions will be difficult, if not impossible, to administer and moreover, could deprive caregivers of vital information necessary to treat the patient appropriately.

Accounting of Disclosures.

The Act provides that a patient is entitled to receive an account of whoever accessed their electronic record, even if such access was for treatment, payment or health care operations. For an inpatient encounter, it would not be uncommon for more than two-hundred people to access various aspects of a patient's record. This would include physicians, nurses, aids, dieticians, phlebotomist, social workers, physical therapists, medical records staff, coders, billing office staff and others. If a patient is provided with a listing of everyone who accessed the patient's record, the provider will then need to

be prepared to explain each individual access. In practice, this could result in substantial and costly efforts on behalf of the provider with little or no apparent benefit to the patient.

Health Care Operation.

The act provides that the Secretary will propose limitations on the use of identifiable health information for health care operations purposes. Currently, there are a wide variety of health care operations purposes that require the use identifiable patient information. I am unsure whether all of these purposes can be identified, let alone reasonably characterized. Further, the burden associated with de-identifying patient information must be considered, not only in terms of the time and effort associated with performing the de-identification, but also in terms of the likelihood that the covered entity will simply choose not to perform the health care operation.

Fundraising.

The Act provides that fundraising would no longer be considered to be part of health care operations. The Act is unclear whether this change has the effect of eliminating the right to perform fundraising as otherwise provided for in HIPAA. In difficult economic times and an era of shrinking reimbursements, fundraising is of critical importance to most providers. Any restriction on fundraising will further frustrate providers' ability to deliver quality health care.

Personal Health Records (PHR) Providers, Health Information Exchanges, Regional Health Information
Organizations and Others.

The Act attempts to address PHR providers, Health Information Exchanges (HIE), Regional Health Information Organizations (RHIO) and other entities that had historically fallen outside the coverage of HIPAA. However, the Act's treatment of each is neither comprehensive nor consistent. Rather than establishing an inconsistent privacy patchwork, a single framework needs to be established to accommodate not only today's requirements, but which also can be extended to cover the rapidly evolving Health IT environment.

Enforcement.

While there has been much criticism of current enforcement strategies, I believe that the manner in which enforcement is performed has been effective. Currently, covered entities can work collaboratively with the Office of Civil Rights (OCR) when privacy issues arise. For example, UPMC has performed self reporting to OCR on a number of occasions. As worded, the Act substantially increases penalties and enforcement. The

Act must ensure that the opportunity to collaborate exists for those covered entities that are dedicated to protecting their patient's privacy.

Audits.

The Act provides for periodic audits of covered entities and business associates. The Act should require that audit criteria be established and published, so that covered entities and business associates can engage internal and external auditors, to conduct audits that would satisfy the Act's requirement.

Studies, Reports and Guidance.

The Act requires that a study be undertaken to assess the privacy and security requirements of non-HIPAA covered entities, and also requires that a report be developed regarding compliance with the Act. Further, the Act requires that guidance on de-identification of protected Health information be provided. While I agree that a study, report and guidance should be undertaken, they should be undertaken in the context of developing a comprehensive privacy and information security framework for health information. This study, report and guidance should be performed in advance of enacting legislation, rather than as a result of the Act.