U.S. Senate Judiciary Committee

"Health IT: Protecting Americans' Privacy in the Digital Age"

January 27, 2009

Responses to Written Questions Requested by the Committee

Submitted by David Merritt

From Senator Hatch:

I strongly support health IT, but believe this must be done very carefully so that we give health care providers the proper incentives to adopt technology without increasing regulatory burdens and costs.

Many health care groups have expressed concerns that requiring new and untested privacy mandates could damage the ability of providers to communicate with patients about treatment options and alternatives. They are also concerned that additional privacy requirements would add costs to the health care system, and actually discourage providers from adopting the very health IT we want them to use.

Do you share these concerns and how would you recommend Congress and the Administration prevent these problems from occurring?

Yes, this is a real concern. A delicate balance needs to be struck between privacy on one hand and treating patients with the most modern tools on the other. In short, we need to find the right balance between privacy at all costs and progress at any cost.

Two issues exemplify the tension: patient consent and data breach notification. Patients should have a legal framework that includes the right of individual consent. Individuals should have the opportunity to opt-out of certain products, services, or notifications and specify how their specific identifiable information can or cannot be shared outside the course of treatment or payment. This consent can be balanced so that it does not impose new, undue burdens on providers, health plans, and other entities.

As I outlined in my written testimony, one way to accomplish this may be through a uniform patient consent form. Such a form could specify standards and instructions that "clearly reflect patients' rights to information in their

medical records and provider confidentiality principles."[1] Such a form could be collected at the time of enrollment in a public or private health plan or before services are delivered.

Patients should also be notified of egregious breaches of privacy and security. And to achieve a balance between informing patients and not complicating the treatment process, the standard for what defines a breach must be set very high. Protections should incorporate a risk-based notification, so that physicians, health plans, and health systems do not notify patients for harmless or inadvertent data sharing. If, for instance, a physician mistakenly sees the record of a patient he or she is not treating, should that qualify as a data breach? Should the patient whose record was seen be notified? The bar should be set very high so that these types of cases do not generate unnecessarily notifications.

The two important issues, as well as many others, should be carefully considered through the rule-making process. There must be a balance between protecting patients and process requirements for health plans, physicians, and other providers.

Question from Senator Specter

You testified that enforcing privacy violations must strike the correct balance between patient privacy and creating a new legal market for frivolous lawsuits. Do you believe that this balance would be disrupted if Congress authorized state attorneys' generals to bring federal HIPAA privacy enforcement actions in federal court for statutory damages and attorneys' fees?

Yes. Under current law, HIPAA may only be enforced by the federal government. This means that HIPAA policy is uniform, that decisions to sue are uniform, and that there no extraneous financial reasons to sue doctors or hospitals. Delegating this responsibility to states and permitting them to re-delegate to private attorneys upsets this equation.

First, it will disrupt national uniformity because each state and each private attorney will be interpreting the law differently. Federal laws should be uniform; with these changes, HIPAA would not longer be. Second, the amendment would interject the private financial considerations of the private attorney into what ought to be a purely legal decision. This is especially so where the attorney is paid on a contingency fee. Third, it will drive up healthcare costs without providing any direct benefit. It may in fact create "defensive information sharing," where doctors treating the same patient are reluctant to share information with each other about that patient. This would actually endanger patients.

---

[1] RTI International, *Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variation and Analysis of Solutions*, July 2007. http://www.rti.org/pubs/avas_execsumm.pdf (Accessed January 24, 2009.)