About
Membership
Government Affairs
Respondent Coop
Information on Demand
CMOR e-Newsletter
What Is Research?
Contact Info

Government Affairs

CMOR :: GA Articles :::

Healthcare Privacy and Healthcare IT
By Howard Fienberg, Director of Government Affairs
November 2007

The development of healthcare information technology (IT) – which could allow comprehensive management of medical information and its secure exchange between health care consumers and providers – also could *spawn new regulatory complications for any survey and opinion researchers collecting or working with any health-related information.*

As the government and private sector push for advanced healthcare IT, privacy activists worry that privacy protections will not keep pace and healthcare IT advocates argue that standardized privacy protections are necessary before the technology can move forward. So what will the future bring for privacy regulations and the survey and opinion research profession's access to data?

While demonstration projects like the Santa Barbara County Care Data Exchange have seen varying degrees of success, the push in the private sector and government to achieve standards for sharing of electronic health information has only grown in strength. CMOR is currently tracking at least 8 bills in Congress on health IT.

In some respects, the federal government is actually taking the lead. At the end of July, the Defense and Veterans Affairs departments established a new "data connection" enabling physicians in either department to access patient records created at the other agency. The Bidirectional Health Information Exchange system merges the Defense's Armed Forces Health Longitudinal Technology Application and the Veterans Health Information Systems and Technology Architecture, allowing physicians from both departments to view medication and allergy profiles, as well as laboratory, radiology and pathology reports.

Meanwhile, Microsoft recently released their HealthVault, a free online tool for patients to organize and track their personal health information in a secure account that belongs solely to the patient. Microsoft sought to avoid controversy by having the Patient Privacy Rights Foundation involved as a consultant from the beginning.

Heightened Privacy Regulation Needed for Standardized Health IT?

Privacy of health information is currently regulated at the federal level by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which requires health care providers (covered entities) to limit disclosure of protected health information (PHI) without the patient's authorization. It also protects individually identifiable health information when it is used, created or maintained for a covered entity by a business associate (which can be survey and opinion research organizations). The law is bureaucratic and quite restrictive, but does not apply to all health information.

Despite the protections the HIPAA Privacy Rule offers, privacy concerns remain high. A recent Government Accountability Office (GAO) report concluded that a comprehensive approach to privacy is required for any national health IT strategy. A "blueprint" for a national healthcare IT network, released by the eHealth Initiative on October 10, agreed.

On July 18, CMOR attended a panel discussion, where all but one of whose participants advocated ***greater federal regulation of healthcare privacy before IT could move forward***:

- *David Merritt (from the Center for Health Transformation and the Gingrich*

Group) agreed that consumers need greater control over their data and their privacy and that further federal regulation is needed.
- *Tom Wilder (from America's Health Insurance Plans)* also spoke of the need for a federal standard, complaining that "having 50 different state laws really causes people a lot of problems."
- *Dr. Deborah Peel (from the Patient Privacy Rights Foundation)* argued that privacy would be served by a single national database for health information and a single national "steward" to transport the information back and forth.
- Only *Dr. Kala Ladenheim (from the National Council of State Legislatures)* dissented, arguing for the benefits of state-by-state innovation and differing levels of enforcement.

On June 12, 2007, the Privacy and Security Workgroup of the American Health Information Community (AHIC), another federal advisory body, publicly stated that all persons and entities that participate in or comprise a health IT network "should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements."

Last year, the National Committee on Vital and Health Statistics, a key national health information advisory committee, made a much more worrisome recommendation to the Secretary of HHS: that the HIPAA Privacy Rule should be extended to include **all** forms of health information, not just those managed by covered entities, and their business associates and contractors, before the development of a nationwide healthcare IT network.

IT standardization may not require privacy law standardization

On the other hand, a study in the BNA Privacy & Security Law Report (March 26, 2007) found no evidence to support the theory that varying state regulations could hinder the development of health IT. The study authors reviewed almost 500 judicial opinions involving access to protected health information (PHI) and privacy of medical information under HIPAA. Their analysis found that only 10% of cases involved situations where the court viewed state laws as more stringent than HIPAA, and none of the cases involved denial of access to providers. They concluded that "a federal effort to legislatively preempt state privacy standards would have limited relevance to the development of interoperable information systems" for health care.

According to Thomas Jeffry, a privacy lawyer and Partner at Davis Wright Tremaine LLP, "HIPAA doesn't provide a specific standard applicable to" healthcare IT, so some doctors, hospitals and providers are concerned about "potential liability over a breach of privacy… However, privacy and security concerns should not be seen as insurmountable obstacles to adoption of IT in health care… early dialogue with a good understanding of the fundamental principles behind privacy and security good practices will go a long way toward reaching consensus."

Bills in Congress

- **The Ten Steps to Transform Health Care in America Act (S. 1783)** is a 113 page monster of a bill. Among many other aspects, it aims to drive the adoption and standardization of healthcare IT, through state and local grants (with private sector matching funds) and demonstration programs. More importantly, it expands the definition of HIPAA "covered entities" to include operators of any "health information electronic database". Such databases will be "*constituted, organized, or chartered for the primary purpose of [or receives valuable consideration for] maintaining or transmitting protected health information in a designated record set or sets*" that are not already otherwise considered covered entities. This legislation does not otherwise change HIPAA privacy regulations.
- **The National Health Information Technology and Privacy Advancement Act (S. 1455)** would provide for the establishment of a national health IT and privacy system, through a new "private, nonprofit corporation" which would administer the system. This "National Corporation for Health Information Technology and Privacy" would be overseen by a new "Office of the National Coordinator for Health Information Technology" within the Department of Health and Human Services.
- **H.R. 2406** would authorize the National Institute of Standards and Technology (NIST), "in consultation with industry and appropriate federal agencies", to develop "technology-neutral infrastructure guidelines and standards," or adopt existing ones, for use by Federal agencies in advancing

the integration of healthcare information enterprises.

- **The Independent Health Record Trust Act (H.R. 2991)** would encourage the development of standardized health IT networks, as well as the creation, use, and maintenance of lifetime electronic health records of individuals in "individual health record trusts" (IHRTs). IHRTs would be legal arrangements, certified by the Federal Trade Commission (FTC), which would handle health records for individuals. The privacy protections for data stored with an IHRT would be relatively similar to the current HIPAA privacy rule for survey and opinion researchers' purposes.
- **The Critical Access to Health Information Technology Act (S. 628)** would award grants to states (which would then grant the money to local entities), with the aim of increasing access to health care in rural areas with improved health IT.
- **The Federal Employees Electronic Personal Health Records Act (S. 1490 and S. 1456**) would require the establishment and maintenance of electronic personal health records for individuals and family members enrolled in any Federal Employee Health Benefit Program plan. Given the large number of participating insurers in the Program, this bill would likely require a majority of the nations' providers to adopt whatever standard of health IT developed by this legislation.
- **The Wired for Health Care Quality Act (S. 1693)** would require government purchases of health IT to meet basic standards on information exchange, as set by the "American Health Information Community" (an existing body which would be codified by this Act). S. 1693 would also authorize five years of competitive matching grants to regional and local health IT networks designed to unite insurers, doctors, hospitals and other health care providers into a single interoperable IT network for information sharing. Similar legislation was passed by the Senate in 2006, but Congress could not agree on any final law.

Conclusion

CMOR will continue to keep the research profession apprised of developments in healthcare IT regulation and their implications for respondent privacy and survey and opinion research.

For more information on HIPAA and healthcare privacy, see CMOR's HIPAA white paper.

Links

- The American Health Information Community: http://www.hhs.gov/healthit/community/background/
- GAO report on health IT: http://www.gao.gov/new.items/d07988t.pdf
- E-Health Initiative "Blueprint": http://www.ehealthinitiative.org/blueprint
- Microsoft's HealthVault: http://www.healthvault.com/
- Patient Privacy Rights Foundation: http://www.patientprivacyrights.org
- The National Committee on Vital and Healthcare Statistics: http://www.ncvhs.hhs.gov
- CMOR on HIPAA and the Privacy Rule: http://www.cmor.org/ga/hipaa_faq.cfm

Disclaimer: The information provided in this article is for guidance and informational purposes only. It is not intended to be a substitute for legal advice. CMOR advises all parties to consult with private legal counsel regarding the interpretation and application of any laws to your business.

"Shielding the Profession"