

A BALANCING ACT:

Patient Privacy Rights and Clinical Practice Needs

By David Hartzband, D.Sc.

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009 as part of the American Recovery and Reinvestment Act to promote the adoption and meaningful use of health information technology. HITECH also modifies the data privacy and security regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and contains a number of provisions focused on the compliance obligations of covered entities and business associates to properly protect patient information.

The HITECH Act modifications, which include provisions that extend the degree to which individuals may restrict disclosures of protected health information, or PHI, have been the focus of intense debate over the past two years. Specifically, the changes permit a patient to elect to restrict from disclosure portions of their personal health information (PHI) if the disclosure is to an insurance plan for payment or administrative purposes, or any health care item or service, that has been paid for in full out of pocket.

The provisions also stipulate that the health care organization or covered entity must limit the disclosure of PHI to a *limited data* set (as defined by HIPAA), or “to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively,” and is responsible for enforcing these restrictions once a patient has indicated their preferences. Finally, the law prohibits the sale of any protected health information without the patient’s consent.

These provisions are clearly intended to protect patient privacy and prevent the inappropriate disclosure of confidential information, and speak directly to the attitudes and concerns of many health care consumers. An August 2010 survey of 2000 adults, conducted by Zogby International for the advocacy group *Patientprivacyrights*, found that 98% of the respondents believed insurers should not be able to sell or share their information without consent; 97%

believed that doctors, hospitals, labs and health technology systems should not be allowed to share or sell sensitive health information without the patient’s consent; and 91% said that individuals should be allowed to decide which doctors and others could view and use their information in electronic health records.

In practice, what the proposed HITECH provisions mean is that patients may specify portions of their PHI, documented in their medical records, which cannot be disclosed. In addition, the health care organization, including the covered entity as well as its business associates, must limit disclosures to the minimum data necessary for the intended purpose, including patient care and treatment.

The Office for Civil Rights in the Department of Health and Human Services is expected to issue final HITECH rules this year, and in a December 2010 statement said that these rules would specifically cover the new HIPAA requirements.

Managing the consent process

The Privacy and Security “Tiger Team” of the Office of the National Coordinator (ONC) has also focused on these provisions, and has made recommendations with respect to consent and information disclosure. These recommendations broadly state that patients should be able to exercise meaningful consent in most disclosure situations, making the provider or provider’s health care organization responsible for: (1) making sure that consent is obtained and maintained, (2) educating and discussing with patients how their information is being shared, and (3) informing the patient when a request concerning PHI disclosure can and cannot be honored.

The proposed changes will require providers to exercise greater care in obtaining and documenting consents of any kind. While consents for direct care are likely to go unchanged in the short term, consents for payment, administrative releases and research and commercial purposes will come under greater scrutiny and

require careful attention. Patients will eventually have greater control over restricting their protected health information and providers will need to be responsible for managing this more complex consent process as well as informing the patient if and when his or her wishes cannot be supported.

Implications for EHRs, care coordination and data exchange

Assuming that the final rules permit patient control over disclosure, any EHR technology deployed by the provider will need to have the capacity for the patient to specify the type of information to be restricted and the purpose for which information should be restricted, and to segment each patient's PHI according to this specification. No existing EHR technology fully allows this, so new functionality will need to be developed, deployed and adopted. The Coalition for Patient Privacy has stated that such segmentation technology exists and has strongly recommended that it be required as part of the HITECH modifications to HIPAA.

As meaningful use unfolds, the Centers for Medicare and Medicaid Services has indicated that Stage 2 meaningful use criteria will most probably make mandatory those criteria now optional in Stage 1. These include patient access and notification, formulary and medication reconciliation capabilities, access to lab data, quality reporting and public health submission. In addition, an emphasis will be placed on exchange of structured data, such as computerized physician order-entry (CPOE) and diagnostic test results. This type of exchange, as well as interaction with public health organizations, will fall under the new more granular consent umbrella.

What about public health reporting, or collection and aggregation of data used for registries? One concern for health care providers is that there be no impediments to meeting prevailing and new public health reporting requirements. Under the law, public health and research use are among the categories exempted from certain provisions related to compensation for data collection, but the law does not exempt an organization from obtaining appropriate consents for the collection and use of data for public health reporting.

Another future consideration concerns the evolution and use of personal health records (PHRs). Many payer and employee organizations now offer PHRs. At the ONC December 2010 public Roundtable on "Personal Health Records: Understanding the Evolving Landscape," it was noted that some organizations already allow individuals to restrict PHI in their personal health records by data element as well as by provider.

Reporting on the roundtable, *Modernhealthcare.com* writes, "Lori Nichols, director of the Whatcom Health Information Network in Bellingham, Wash., said it affords patients "very detailed blocking" capabilities to mask highly sensitive [information] by data element and provider," using role-based access (i.e., authorizing or restricting access to information based on an individual's role in an

organization). Meanwhile, roundtable discussant Colin Evans, the CEO of Dossia, a PHR provider, described his company's aim as being to "create a privacy environment in which secondary use of a patient's health care information is not permitted." Potentially, this level of patient control could mean that some members of a medical home team could see certain data while other members could not; this could have important ramifications for full, comprehensive and continuous patient care and treatment.

It is clear that future regulation will take into account the expressed need for patients to have more granular control over how their protected health information is used and who gets to see it. It is also clear that at some point, if and as this control is extended to the restriction of specific data elements (including defined aspects of medication history, or treatment for specific conditions), there could be tension between the wishes of the patient and the clinical judgment of the treating provider.

Primary care medical homes assume and require the greatest possible degree of coordination of care, and such coordination of care requires the exchange of information. To the extent that some protected health information may be restricted at the discretion of the patient, providers need to be aware of what data they are looking at and think about how to best ensure continuous, comprehensive care.

We have a long way to go before EHR technology enables refined PHI segmentation, but we cannot afford to ignore the possibility of its availability. In the meantime, health centers need to become knowledgeable about the more complex consent requirements under current and proposed regulations and to work with their vendors to make sure they will be able to meet the requirements and address the concerns of their patients while continuing to offer the highest possible standards of care.

David Hartzband, D.Sc. is the Director of Technology Research at the RCHN Community Health Foundation.

- 1 For disclosure requirements see HITECH 42 CFR 17935 restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format. Section 13405
- 2 HITECH Act, "PROHIBITION ON SALE OF ELECTRONIC HEALTH RECORDS OR PROTECTED HEALTH INFORMATION" section 13405 (d)(1) and 13405 d(2)
- 3 2000 Adults' Views on Privacy, Access to Health Information, and Health Information Technology "<http://patientprivacyrights.org/wp-content/uploads/2010/11/Zogby-Result-Illustrations.pdf> See also "Patients Want Control of e-Records" <http://www.zogby.com/Soundbites/readclips.cfm?ID=19716>
- 4 See Steve Ganz, "Security Architecture," May 28, 2010, http://blog.securityarchitecture.com/2010_05_01_archive.html
- 5 Joseph Conn, "Health-record providers take aim at privacy concerns" <http://www.modernhealthcare.com/article/20101206/NEWS/312069979/>, December 6, 2010
- 6 Ibid. See also *ihealthbeat* "Panelists Say Privacy Policies Bar Access to Personal Health Records" December 7, 2010, <http://www.ihealthbeat.org/articles/2010/12/7/panelists-say-privacy-policies-bar-access-to-personal-health-records.aspx>