

ModernHealthcare.com

STIMULUS BROADENS PRIVACY DISCLOSURE ACCOUNTING

By Joseph Conn / HITS staff writer

Posted: March 2, 2009 - 5:59 am EDT

Patient-privacy advocates have plenty to cheer about in the American Recovery and Reinvestment Act of 2009 signed into law last month by President Barack Obama.

Hospitals, physician offices, health plans, pharmacies, claims clearinghouses and other so-called "covered entities" under the Health Insurance Portability and Accountability Act of 1996, as well as their business associates—if they use electronic health-record systems—will be required to provide patients with a much broader accounting of the disclosures they make of a patient's protected healthcare information.

In addition, the new law also will require covered entities to honor a patient's request not to disclose to payers treatment information if the patient pays out-of-pocket for healthcare.

Both new privacy requirements will go into effect one year after enactment, according to the California Office of Health Information Integrity. Under the current HIPAA privacy rule, covered entities have only a limited duty to account for disclosures of patient information, since releasing records for the main uses—treatment, payment and other healthcare operations—are exempt from the disclosure accounting requirement.

Under the stimulus law, covered entities must provide a patient an accounting of disclosures, even for treatment, payment and other healthcare operations. It's "a very positive step for privacy," wrote Robert Gellman, a Washington lawyer and privacy consultant, in an **18-page analysis of the privacy provisions of the new law**.

Under the new law, the requirement was dropped that covered entities provide an accounting of disclosures by their business associates. And yet, the new law requires business associates to comply with privacy requirements in an equal manner as covered entities themselves, so businesses associates stay on the hook for tracking and reporting what they do with patient information.

Those requirements will afford patients broader capabilities in tracking who has seen their medical information, Gellman said, but it also could make patients, covered entities and business associates all work harder. "The process isn't entirely clear," he said. "The covered entity can say, 'Here are the disclosures that we made, and here is a list of all of our business associates and you go talk to them.' The rulemaking can help a lot with this."

Forcing patients to obtain disclosures through multiple tiers of business associates will be cumbersome and would have been unnecessary, Gellman said, if Congress had simply left alone the requirement that a covered entity had the responsibility to be the patient's point of contact for both its own disclosures and those of its business associates.

"That's going to have to be done automatically, or there are going to be lawsuits," Gellman said. "It's great for privacy and it may turn out to be a necessary model for other requests, but it's going to take careful planning in any electronic system. I have no doubt that it's doable, but doable and doing it is something else."

Patient controls over the electronic flow of their information already are firmly established by IT programs in Canada and Europe..

Several companies offer technology overlays that specifically provide patient-consent management and disclosure accounting functions—Health Information Protection and Associated Technologies, or HIPAAT, of Mississauga, Ontario, and Naples, Fla., which participated in a demonstration in December 2008 along with IBM Corp. of a national health information network implementation; and **Private Access, Irvine, Calif., which won the "hot products" award at the Towards an Electronic Patient Record trade show last month in Palm Springs, Calif.**



Callahan

Terry Callahan, managing director of HIPAAT, said the company's system could handle creating consent directives that would block transmission of specific patient data to payers. It also can block data flow to specified providers, do disclosure audits and breach notifications as well.

"If somebody says, let's send it (a breach notification) out to the patient, we just change the e-mail address," Callahan said. "These are things we have been doing for some time. We can also control who is allowed to see the consent directive itself."

One other item under the new law might cause a bit of a scramble. It is a requirement that essentially drags regional health information organizations and exchanges, electronic-prescribing gateways and at least some vendors of personal health-record systems under the HIPAA tent.

Those that exchange patient information with a covered entity or their business associates must comply with the requirement that they sign business associate agreements with the covered entity and "shall be treated as a business associate of the covered entity," and must comply with HIPAA privacy and security rules in the same manner as covered entities.



Gellman