Recovery and Privacy: Why a Law about the Economy Is the Biggest Thing since HIPAA

by **Dan Rode**, MBA, CHPS, FHFMA

When Congress passed the final stimulus bill in February, healthcare received more than just money. Among the billions were major new privacy and security requirements.

Those who followed the Congressional debates on the stimulus bill in the mainstream press probably were surprised to find that the final product—the American Recovery and Reinvestment Act of 2009, or ARRA—contains 21 pages dedicated to healthcare information privacy. Why would a law intended to jumpstart the economy include the most significant collection of privacy regulations since HIPAA?

The answer is found in the act's title XIII, often referred to as HITECH, which provides funding for the adoption of healthcare IT. ARRA contains privacy legislation because Congressional members understood that without addressing ongoing privacy issues, a comprehensive health IT bill would not pass.

If the ARRA provisions were a surprise, few in healthcare should be taken unaware by the topics. The new requirements result from debate that has occurred since the HIPAA privacy requirements became effective in 2003. The ARRA provisions reflect discussion and compromise that continued until the final hours before the US Senate finally agreed to an overall package.

The provisions still require the detail that will come in final rules, which will begin to appear this summer. But the changes ARRA outlines touch a wide range of healthcare activities, and they introduce dramatic changes in how organizations manage their privacy practices.

Changes within HHS

To be clear, the ARRA language signed into law on February 17 lays out Congress's intent. The Department of Health and Human Services (HHS) must now propose and adopt final regulations that establish the ground rules for conforming to the intent of the law.

HHS also must respond to administrative changes introduced by the law. ARRA establishes the Office of the National Coordinator for Health Information Technology (ONC) as a permanent office and defines its purpose regarding the development of the national health information technology infrastructure. ONC has lacked permanent status since its creation by executive order in 2004.

ARRA requires ONC to appoint a privacy officer to serve in an advisory role on policy and standards issues. HHS must appoint privacy officials in each of its regional offices to work with healthcare entities and consumers. The changes do not supplant the role of the Office for Civil Rights as the oversight agency for privacy or the Centers for Medicare and Medicaid Services, which retains oversight over HIPAA security.

Select Due Dates for ARRA Provisions

Many of the interim rules necessary to establish provision details will appear in the coming year, with provisions taking effect over the next three years. Some of the first provisions to take effect are related to breach

notification and disclosure.

Description	Responsible Party	Due (no later than)	Effective
Interim final rule on breach requirements: HIPAA covered entities	HHS secretary	August 2009	Breaches discovered 30 days after publication
Interim final rule on breach requirements: entities not covered by HIPAA (e.g., PHR vendors)	Federal Trade Commission	August 2009	Breaches discovered 30 days after publication
Regulation on data to be provided in accounting for disclosure related to EHRs	HHS secretary	August 2009	January 2011 for new systems; January 2014 for existing systems

Source: AHIMA. "Analysis of Health Care Confidentiality, Privacy, and Security Provisions of the American Recovery and Reinvestment Act of 2009, Public Law 111-5." March 2009. Available online at www.ahima.org/dc.

A Federal Law on Breach Notification

ARRA establishes the first federal requirements on health data breach reporting and notification. Further, it extends those requirements past the traditional covered entities under HIPAA to include business associates and noncovered entities that handle protected health information (PHI) as defined in the law. This is the first federal acknowledgment that PHI should be protected no matter where it resides.

HHS will continue to oversee covered entities, and it now adds business associates to its oversight. Noncovered entities involved in breaches of "nonsecure" data will be overseen by the Federal Trade Commission for the foreseeable future. ARRA calls for HHS and the trade commission to cooperate.

The breach provisions will generate some of the first requirements to come out of ARRA, including guidance related to securing data held in personal health records. The law requires the HHS secretary to issue final interim regulations by August. The requirements will apply to breaches discovered 30 days on or after the publication of the interim rule.

Entities not covered by HIPAA will also be subject to the HHS secretary's guidance related to "nonsecured" data; however, the FTC will issue the final rules. The timetable will be the same. ARRA specifically identifies vendors or operators of personal health records as subject to FTC regulations when they are not covered under HIPAA.

Currently more than 40 states have data breach notification laws. The arrival of federal law will challenge many entities to address both the ARRA breach requirements and their own state requirements. As with HIPAA, the new ARRA provisions do not preempt state requirements that are stricter than the federal requirements.

New Obligations for Business Associates

ARRA increases the obligations of business associates as identified under HIPAA, subjecting them to select HIPAA privacy and security regulations. These include the need for administrative, physical, and technical safeguards as well as policies and procedures and documentation requirements.

Business associates also will be obligated to comply with privacy requirements on use and disclosure and "application of knowledge elements"—that is, they will be required to act on knowledge they may have of a covered entity's lack of compliance, just as a covered entity is currently responsible for acting on a business associate's failure to comply. Business associates will be subject to the tougher penalties spelled out in ARRA.

As noted, ARRA's data breach notification provisions extend directly to business associates, who must notify covered entities in the event of any data breaches they experience. Covered entities may request that their business associates report the events themselves.

ARRA requires the secretary of HHS to issue annual guidance on the "most effective and appropriate technical safeguards" for carrying out the security requirements. While this requirement is addressed to business associates, adherence to the guidance will likely be expected of all HIPAA covered entities.

ARRA also extends both its own requirements and the HIPAA security and privacy requirements for business associates to health information exchange organizations, regional health information organizations, e-prescribing gateways, and other organizations that transmit PHI.

Once final rules are available, covered entities will have to renegotiate their contracts accordingly with each of their business associates.

More Consumer Control on Disclosure

ARRA permits consumers to restrict a covered entity's ability to disclose information to health plans under HIPAA's payment and operations provisions on services for which the individual pays out of pocket and in full. While the number of such requests may be minimal, fulfilling them will likely be complicated, depending on an entity's operations structure.

An individual's request could encompass the entire encounter, visit, or admission, or it might represent only a portion of the services performed in the encounter. Covered entities will have to be aware of data flows for claims and medical records or data involved in payment or treatment.

ARRA also increases a covered entity's obligation to use the HIPAA limited data set when responding to requests for PHI. When the limited data set does not meet the need for disclosure, an entity can now make a determination of what constitutes "minimum necessary."

This provision requires the secretary of HHS to issue guidance on what constitutes "minimum necessary," a point of contention for some time, particularly between providers and health plans.

A third disclosures provision requires covered entities that use electronic health record systems to account for all disclosures upon consumer request. This includes disclosures for treatment, payment, and operations, which are exempted under HIPAA. The secretary of HHS will define a standard for the accounting and will issue regulations for compliance. The effective dates are staggered depending on when an entity purchased its system. The earliest date is January 1, 2011. The HHS secretary has the leeway to extend the effective dates up to two years.

ARRA also addresses the fees an entity may charge for providing a copy of an individual's record. The law explicitly permits individuals to obtain an electronic copy of their records from providers with electronic systems, and it enables the provider to impose a fee for the labor associated with fulfilling the request. Regulations on these release of information issues are called for by summer 2010.

Better Defining Marketing and Fund-Raising

Congress also used ARRA to address concerns about HIPAA's marketing and fund-raising requirements regarding PHI. The HHS secretary is directed to define the scope of fund-raising that might be considered a part of healthcare operations and how it must be communicated to the individual.

ARRA continues to prohibit the use of PHI for marketing, but it adds clarification as to when such communication might be permitted outside of healthcare operations. It calls for further regulation to define "reasonable in amount" related to some

reimbursement that might be received by a covered entity or business associate.

Increased Enforcement

The law takes a number of steps to improve enforcement of both HIPAA and its own forthcoming regulations. It also clarifies that individuals, not just entities, are subject to penalties. The clarification is meant to override a previous Department of Justice letter suggesting that individuals could not be convicted under HIPAA.

The new enforcement provisions raise the specter of "noncompliance due to willful neglect," and they add penalties as high as $1.5 million per year to the mix of enforcement actions.

Previously, any monies collected under HIPAA penalties were placed in the government's general coffers; ARRA now calls for the penalties or monetary settlement collections to be given to the Office for Civil Rights. Individuals whose PHI was involved in the actions may also receive a share of the penalty or settlement.

ARRA directs the comptroller general to submit recommendations for such sharing to the HHS secretary and for the secretary then to issue regulations. This is to happen within three years. All new enforcement penalties and sharing provisions are retroactive to February 17, 2009—the law's enactment date—except for the action under "willful neglect."

ARRA empowers state attorneys general to enforce HIPAA, adding another avenue for enforcement. The provision received much publicity at the time, but it likely will see limited use. Attorneys general may only enforce HIPAA in restricted situations, and they are limited in the damages they can impose.

The HHS secretary now must periodically audit covered entities and business associates and post reports on breaches for public scrutiny. The secretary is also obligated to report to Congress on breaches, compliance, and the overall impact of ARRA on the healthcare industry. The Office for Civil Rights is required to develop and maintain a "multi-faceted national public education initiative to enhance public transparency" regarding the use of PHI as well as individual rights regarding its use.

With ARRA the federal government has made a significant financial investment to increase the use and exchange of digitized health information. That investment required renewed commitment to ensuring the privacy and security of that information. Working through the law's new provisions will challenge a healthcare industry already struggling with great change. HIM professionals helped make HIPAA work. Now they must begin the task of doing the same for the ARRA provisions.

For More Information

www.thomas.loc.gov

- The Library of Congress's Thomas Web site offers the law's full text. Search for public law 111-5.

www.ahima.org/dc

- AHIMA breaks out the law's privacy and security provisions by section and identifies the core issues. A separate analysis identifies the reports and their due dates called for in the act. See "Regulation Analysis."

Dan Rode (dan.rode@ahima.org) is vice president of policy and government relations at AHIMA.

Article citation:
Rode, Dan. "Recovery and Privacy: Why a Law about the Economy Is the Biggest Thing since HIPAA" *Journal of AHIMA* 80, no.5 (May 2009): 42-44.