LegalNotes

Volume1 **Issue**2 **Part**II

LegalNotes is a regular online *Aligning Forces for Quality* (AF4Q) publication that provides readers with short, readable summaries of developments in the law that collectively shape the broader legal environment for efforts to improve quality, reduce health care disparities, and improve the transparency of price and quality information.

The American Recovery and Reinvestment Act of 2009
Part II - Privacy Provisions

Melissa M. Goldstein, J.D.
Lara Cartwright-Smith, J.D., M.P.H.
Sara Rosenbaum, J.D.

On February 17, 2009, President Barack Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA), also called the "Recovery Act," into law.[1] ARRA provides hundreds of billions of dollars in new health and health care spending, including more than $19 billion to support and promote the adoption of electronic health records. In three short issue briefs, we address key areas of the law: health information technology, privacy and comparative effectiveness.

This second brief of the **Legal**Notes three-part series on ARRA focuses on its reforms to existing laws related to health information privacy and security, particularly its revisions to the Health Insurance Portability and Accountability Act (HIPAA). The new provisions broaden the reach of and strengthen existing privacy and security standards and add new provisions related to enforcement. The legislation:

- Strengthens the level of individual control over information contained in an electronic health record (EHR);
- Broadens the definition of who is a business associate of covered entities and increases business associate duties;
- Creates new notification duties in the event of security breaches;
- Expands the accounting that covered entities must provide individuals regarding health information disclosure;
- Places new restrictions on marketing, fundraising and the sale of protected health information (PHI);
- Requires the development of guidelines regarding the use of limited data sets and de-identified data; and
- Increases penalties for violations and adds new enforcement provisions.

Individual Control Over and Access to PHI

The Recovery Act specifies that when a health care provider or other HIPAA-covered entity uses an EHR containing an individual's PHI, the individual will have the right to a copy of his or her record in an electronic format, and to have the record sent directly to another person.[2] ARRA thereby incentivizes the creation of personal health records (PHRs), identified by many experts as an essential step in making securely-managed personal health data more broadly accessible than is currently the case in provider-owned records. The individual may not be charged more than actual labor costs to respond to this request.

In addition, the Recovery Act provides individuals more power to restrict the disclosure of their PHI. Currently under HIPAA, providers can choose whether to agree to follow an individual's request not to disclose his or her information (but are bound by any

Legal Barriers, based at The George Washington University School of Public Health and Health Services, provides technical assistance for *Aligning Forces for Quality,* a national initiative of the Robert Wood Johnson Foundation.

agreement they make). ARRA makes provider compliance with a request mandatory (unless disclosure is otherwise required by law) if the disclosure is to a health plan for purposes of carrying out payment or health care operations (not treatment), and if the PHI pertains to a health care item or treatment for which the provider was paid out-of-pocket in full. This provision does not apply to de-identified patient information.

Increased Duties for Business Associates and Other Entities

The application of HIPAA's privacy and security protections to business associates of covered entities has been controversial since its passage in 1996. Until now, business associates have not been subject to the detailed requirements of HIPAA privacy and security rules. ARRA addresses this issue and also imposes new requirements on vendors of PHRs and other non-HIPAA entities.

a) Application of HIPAA to business associates[3]

Under ARRA, business associates will now be subject to HIPAA's security requirements. The Recovery Act does not apply the full range of HIPAA privacy standards to business associates, but does prohibit business associates from disclosing PHI outside of the terms of a HIPAA business associate contract. The privacy and security requirements created by ARRA will apply to business associates, and business associates will now be subject to the same civil and criminal penalties applicable to covered entities under HIPAA.

b) Business associate contracts required for PHR vendors and other non-HIPAA entities[4]

ARRA clarifies that health information exchanges and other organizations that transmit PHI to a covered entity (or its business associate) and require routine access to PHI are business associates and must enter into business associate contracts with the covered entity. The same applies to vendors that contract with a covered entity to allow the covered entity to offer a PHR.

Privacy and Security Breach Notices

Many states have recently passed laws requiring businesses to notify consumers of breaches of the security of their personal information in electronic databases. HIPAA, however, had no strict notification requirement. ARRA changes this by requiring covered entities to notify individuals whose unsecured PHI has been disclosed as a result of a privacy or security breach.[5] In certain cases, the covered entity must also notify the Secretary of the U.S. Department of Health and Human Services and the general public. If a breach is discovered by a business associate, it is required to notify the covered entity of the breach, including the identification of each individual who is reasonably believed to have been affected by the breach. The new federal requirements do not preempt state notification requirements that are more restrictive, so covered entities will likely have to comply with both. The requirements do not apply to certain unintentional disclosures of PHI. ARRA also applies a similar breach notification requirement on vendors of PHRs and other non-HIPAA entities.[6]

Expanded Accountings of Disclosures

Under current HIPAA regulations, covered entities are required to provide an accounting of certain disclosures of PHI to individuals who request it, but they do not need to account for disclosures of treatment, payment or health care operations. ARRA expands an individual's right to an accounting of disclosures to include those made through an EHR during the three-year period prior to the request, including disclosures made for treatment, payment and health care operations. Because performance measurement and health care quality improvement are essential dimensions of health care operations, presumably such uses would be covered by the disclosure accounting provisions.

New Restrictions on Marketing and Fundraising

ARRA clarifies that patient consent is required for communications by a covered entity or business associate that encourage patients to purchase or use a product or service (i.e., marketing).[7] Communications will still be acceptable when they describe only a drug or biologic that is currently prescribed for the patient and when any payment received by the covered entity in exchange for making the communication is reasonable. In addition, ARRA allows providers to engage in fundraising activities using a patient's PHI as long as they provide an opportunity for the patient to opt out of solicitations.

Restriction on the Sale of PHI

Except in the area of marketing, HIPAA does not prohibit a covered entity from being paid for PHI as long as the disclosure is otherwise permitted. ARRA now generally prohibits a covered entity or business associate from selling patients' PHI without specific authorization, with certain exceptions including payment for treatment, certain public health activities, research or other activities as specified by the Secretary.[8]

Limited Data Sets and De-identified Data

ARRA specifies that covered entities will automatically be in compliance with HIPAA when they limit the PHI information used, disclosed or requested to the "limited data set" (as defined by the HIPAA Privacy Rule in relation to anonymity), or if needed by the covered entity to the "minimum necessary" to accomplish the intended purpose.[9] Covered entities and business associates will have discretion to decide what constitutes "minimum necessary," and de-identified information is exempt from the disclosure limits.

The Secretary is required to issue guidance on what constitutes "minimum necessary" within 18 months, and must take into consideration that "minimum necessary" should encompass the information necessary to improve patient outcomes and to detect, prevent and manage chronic disease. The Secretary is also required to develop guidance on how best to implement HIPAA's requirements for the de-identification of PHI.[10]

Improved Enforcement

ARRA improves HIPAA privacy enforcement, including new enforcement approaches, tiered penalties based upon the nature and extent of a violation and the harm caused, and the empowerment of state attorneys general to bring civil suits in federal court to recover damages on behalf of states' citizens. Increased penalties for violations of HIPAA are effective immediately, while penalties for violations of ARRA's provisions will be effective in two years.

Implications for Data Collection and Reporting

As a result of ARRA, organizations that use patient information for quality improvement activities or public reporting may be subject to new privacy and security requirements. Even if the information received does not include individual patient data, it may still be considered PHI that does not meet the definition of de-identified under HIPAA. Organizations receiving data from providers and payers who are covered entities under HIPAA may be subject to additional requirements as business associates. Therefore, AF4Q grantees and other organizations should look closely at their data use agreements and monitor their data management practices to ensure that they are using patient data in compliance with HIPAA and ARRA. In addition, ARRA requires the Secretary to consider expanding HIPAA's privacy and security rules to entities that are not currently covered under the law. This means that in the future, even more types of organizations may be subject to these laws.

Conclusion

Congress made the adoption of health information technology one of the major policy priorities of ARRA, and in so doing, revised and expanded health information privacy law as well as the groups to which it applies. Under the new law, business associates of health care providers and other entities that create or use PHI will need to follow HIPAA's privacy and security rules, including the stricter provisions added by ARRA. In addition, ARRA requires business associate agreements for a broader variety of entities, which may include local data collection and reporting entities. As described in the first brief of this series, federal policy is encouraging greater use of EHRs as part of a larger focus on transparency in health care. Increased transparency carries greater risk of improperly disclosing PHI. ARRA's privacy provisions reflect Congressional recognition of this risk.

---

[1]The American Recovery and Reinvestment Act of 2009 (ARRA), Public Law 111-5, 111th Cong., 1st sess. (2009).

[2]ARRA § 13405.

[3]ARRA §§ 13401, 13404.

[4]ARRA § 13408.

[5]ARRA § 13402.

[6]ARRA § 13407.

[7]ARRA § 13406.

[8]ARRA § 13405.

[9]*Id.*

[10]ARRA § 13424.