7-28-2009

How the American Recovery and Reinvestment Act of 2009 Changed HIPAA's Privacy Requirements

Corrine Parver
American University Washington College of Law, cparver@wcl.american.edu

On The Front Lines

How The American Recovery and Re[illegible]ment Act of 2009 Changed HIPAA's Privac[illegible] Requirements

by Corrine P. Parver, Esq. & Savannah Thompson-Hoffman

The 2009 economic stimulus bill, known as the Amer[illegible] Recovery and Rein[illegible]vestment Act (ARRA),[1] significantly affects the health care industry by imposing more stringent and expansive requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2] privacy and security provisions, most especially on key players in the health care industry while simultaneously strengthening the enforcement of such provisions. Title XIII of Division A and Title IV of Division B of ARRA collectively are known as the "HITECH Act." Because the majority of ARRA's changes to HIPAA appear in Subtitle D of Title XIII of ARRA, entitled "Privacy," Subtitle D will be the primary focus of this article, which highlights ARRA's major changes to the HIPAA privacy and security provisions and explores the implications of these sweeping changes for the health care industry.

Direct Application of HIPAA's Privacy and Security Provisions to Business Associates

Perhaps the most sweeping change made by ARRA is its imposition of HIPAA obligations and liability on business associates. Section 13401 of ARRA makes a major change in the treatment of business associates by extending the application of the HIPAA physical,[3] technical,[4] and administrative security[5] provisions to business associates, provisions that previously applied only to covered entities.[6] Section 13404 further restricts the ability of business associates to use and disclose protected health information by extending the application of HIPAA privacy provisions[7] to business associates.

Covered entities are health plans, health care clearinghouses, and health care providers that transmit electronic health information.[8] Business associates contract with covered entities to perform functions or services on behalf of the covered entities "involving the use or disclosure of individually identifiable health information,"[9] such as: "legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services."[10]

Prior to the enactment of ARRA, HIPAA privacy and security rules applied only to covered entities.[11] Business associates were not directly covered by HIPAA but were obligated to comply with privacy rules to the extent required in their contracts with covered entities.[12] If a business associate breached the terms of the contract, known as the business associate agreement, thereby violating HIPAA, the business associate was liable only to the covered entity for breach of contract and was not subject to federal penalties.

Sections 13401 and 13404 impose direct liability on business associates for violations of HIPAA security and privacy provisions, respectively, and erase an important distinction between business associates and covered entities by subjecting business associates to the same civil and criminal penalties that apply to covered entities for HIPAA violations. Thus, all business associate agreements between business associates and covered entities must be updated to reflect ARRA's new privacy and security requirements.

Expanded Definition of Business Associate

Section 13408 broadens the definition of business associate for the purposes of HIPAA to include organizations that "provid[e] data transmission of protected health information" to covered entities and that "requir[e] access on a routine basis to such protected health information."[13] Health Information Exchange Organizations, Regional Health Information Organizations, E-prescribing Gateways, and vendors that "contrac[t] with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record" are examples of business associates under ARRA's expanded definition.[14] One implication of this expanded definition of business associate is that, under ARRA, these organizations are now required to enter into business associate agreements with covered entities and are subject to the same penalties as covered entities.

Stricter Breach Notification Requirements

Section 13402 imposes federal breach notification requirements on both covered entities and business associates. Section 13402(a) requires a covered entity to notify an individual if there has been a breach or reasonably suspected breach of that individual's unsecured protected health information (PHI). Section 13402(b) requires a business associate to notify a covered entity in the event of a breach or suspected breach of an individual's PHI.

A breach is defined as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information."[15] Three main exceptions exist to this definition. First, a breach does not occur when an unauthorized person who receives PHI is unable to reasonably retain the information. Second, a breach does not occur if an "unintentional acquisition, access, or use" of PHI occurs within the scope of employment of an employee of a covered entity and the information is "not further acquired, access, used, or disclosed by any person."[16] Finally, a breach does not occur if the disclosure of PHI is both inadvertent and is from "an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate" to a "similarly situated individual at the same facility."[17] Importantly, the information must not be "further acquired, accessed, used, or disclosed by any person."[18]

A breach is considered "discovered" on the first day it is known or should reasonably have been known to have occurred.[19] Breach notifications are required to be made "without unreasonable delay" and not later than 60 days after discovery of the breach.[20] The burden of proof is on the covered entity to demonstrate that all required notifications of breach were made and explain the reasons for any delay in notification.

In the event of a breach, there are a variety of methods of notice under Section 13402(e) that are required depending upon the circumstances and the number of individuals affected. Generally, an individual must be notified by first-class mail if his or her unsecured PHI has been breached.[21] If notification by mail is not possible, a substitute form of notice shall be provided such as a phone call or email. If the PHI of ten or more individuals has been breached and there is insufficient contact information, the covered entity must post a conspicuous notice on its web site or place a notice in the local media.[22] In addition to notifying the affected individual of the breach, the covered entity also must keep a log of all breaches and submit annual documentation of such breaches to the Secretary of the Department Health and Human Services (HHS).[23]

If the PHI of more than 500 individuals of a state is breached, the covered entity responsible for the breach must provide notice to prominent media outlets as well as immediate notice to the Secretary of HHS. In such a situation, the Secretary is required to list the covered entities involved in the breach on HHS's website.[24]

The breach notification should include five pieces of information – (1) a brief summary of what happened, (2) a description of the types of unsecured PHI involved in the breach, (3) a description of what the covered entity is doing to investigate the breach and prevent further breaches, (4) the steps the affected individual should take to mitigate the harm resulting from the breach, and (5) contact information to allow the individual to learn more information about the breach incident.[25] Vendors of personal health records also must notify an individual if there has been a breach of that individual's unsecured personal health record. Additionally, vendors must notify the Federal Trade Commission in the event of a breach.[26]

Encryption and Data Destruction Provide Safe Harbor from Breach Notification Requirement

The breach notification requirement is only triggered when the PHI that is breached is unsecured. Health information is "secured" if it is rendered "unusable, unreadable, or indecipherable to unauthorized individuals" using a methodology that the HHS Secretary approved.[27]

On April 27, 2009, HHS published guidance, as required by Section 13402(h) of ARRA, specifying the technologies and methodologies that render PHI secured.[28] Under the guidance, covered entities and business associates may use encryption or data destruction, among other methods, to secure PHI so that the notification requirement is not triggered if the information is breached. "While covered entities and business associates are not required to follow the guidance, the specified technologies and methodologies, if used, create the functional equivalent of a safe harbor and, thus, result in covered entities and business associates not being required to provide the notification otherwise required by Section 13402 in the event of a breach."[29] Covered entities and business associates nevertheless must comply with applicable state regulations regarding the breach of PHI as well as HIPAA's requirement that any harmful effects of the breach be reasonably mitigated.[30]

Expanded Individual Rights

ARRA greatly expands the rights of individuals under HIPAA. For the first time, covered entities have an obligation to comply with an individual's request to restrict the disclosure of PHI if the disclosure is not for the purposes of treatment, and the information "pertains solely to a health care item or service for which the health care pro-

vider involved has been paid out of pocket in full."[31] Prior to ARRA, individuals could request restrictions on the disclosure of their PHI, but covered entities were under no obligation to comply.[32] This new provision imposes an administrative burden on health care providers by requiring them to separate certain information (for services which have been paid for out of pocket in full by an individual) from the rest of an individual's record.

Section 13405(c) further expands the rights of individuals by giving them the right to request a description of all disclosures of their PHI stored in an electronic health record made during the three years prior to the request.[33] Prior to ARRA, individuals had the right to request an accounting of the disclosures of their PHI by a covered entity or its business associates during the six years prior to the accounting request, but covered entities were not obligated to account for disclosures for treatment, payment, or health care operations. While Section 13405(c) imposes a burden on covered entities to adopt a new accounting method to track each disclosure of PHI, including disclosures for treatment, payment, and health care operations, it "represents a major change in the transparency of health data uses and flows."[34]

Section 13410(c) reinforces the rights of individuals by requiring the establishment of a methodology to distribute to an "individual who is harmed by an act that constitutes an offense [under Subtitle D]... a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense."[35] While individuals do not have a private cause of action to vindicate their own rights under HIPAA, ARRA now recognizes harmed individuals by allowing them to share in part of the monetary penalty collected.

Restrictions on the Sale of Protected Health Information and Marketing Communications

Section 13405(d) prohibits the sale of electronic health information without patient authorization except in certain circumstances. These circumstances include when the exchange of information is for: public health activities, research, treatment of the individual, the health care operation, or to provide the individual with a copy of his or her PHI. This provision effectively "shut[s] down the secondary market that has emerged around the sale and mining of patient health information by prohibiting the sale of an individual's health information without [his or her] authorization."[36]

ARRA "clarifies that a marketing communication by a covered entity or business associate about a product or service that encourages the recipient to purchase or use the product or service may not be considered a health care operation unless the communication is for a health-care related product or service, or relates to the treatment of the individual."[37] Section 13406 requires written fundraising communications to "provide an opportunity for the recipient of the communications to elect not to receive any further such communication."[38]

Penalties and Protections: Strengthened Enforcement of HIPAA with Increased Penalties

ARRA sharpens the teeth of HIPAA provisions by increasing civil penalties and expanding the scope of enforcement opportunities. Section 13410 amends HIPAA by "replacing the existing civil monetary penalties with four tiers of penalties, the highest of which would impose a fine of $50,000 per violation and up to $1,500,000 for all such violations of an identical requirement or prohibitions during a calendar year."[39] The four tiers are differentiated based upon the knowledge and intent of the person who violated the provision. Persons who "did not know (and by exercising reasonable diligence would not have known) that they were violating a provision, fall into the first tier. The second tier includes persons whose violations were "due to reasonable cause and not willful neglect." Persons who engage in violations due to willful neglect but who correct the violation within a specified time fall into the third tier. Finally, the fourth tier includes persons whose violations are due to willful neglect and who fail to correct the violation within a specified time.[40]

Various members of the health law bar have expressed some puzzlement over the meaning of ARRA's tiered penalty provisions. While some have interpreted Section 13410(d)(1)(A) to ascribe the maximum 1.5 million dollar penalty to unwitting violations, logic dictates that it would be inconsistent with the plain meaning of the statute to apply the same penalty to unwitting violations as those violations resulting from willful neglect.[41] If a violation is due to "willful neglect," the Secretary is required to investigate formally the situation and impose a civil monetary penalty. Moreover, the Secretary is required to "perform periodic audits to ensure compliance with the HIPAA privacy and security standards" and the requirements of Subtitle D.[42]

Finally, ARRA amends HIPAA by authorizing state attorneys general to bring a civil action in federal court on behalf of individuals who were "threatened or adversely affected by any person who violates a provision of HIPAA against individuals who threaten" an interest of one or more of the residents.[43] This change will likely contribute to greater attention to enforcement of HIPAA at the state level.

Enhanced Guidance and Education

Section 13401 requires the Secretary, in consultation with stakeholders in the health care industry, to issue annual guidance on "the most effective and appropriate technical safeguards" for protecting electronic health information.[44] Section 13403 requires the Secretary to appoint an individual in each HHS regional office to "offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities" related to health information privacy and security.[45]

Because the Office for Civil Rights (OCR) currently provides guidance, it is likely that a regional contact will be able to provide more personalized and tailored guidance and advice to local entities. Section 13403 requires OCR to create a national

education initiative to teach individuals about the permissible uses of their PHI and their rights under HIPAA. This initiative will "enhance public transparency" and empower individuals to ensure that their PHI remains secure.[46]

Ramifications of ARRA's Changes to HIPAA for the Health Care Industry

ARRA increases the rigor and broadens the scope of HIPAA compliance. These broad new requirements necessitate a variety of expensive and time-consuming changes by covered entities, business associates, and vendors to ensure compliance.

Covered entities, business associates, and vendors will need to update their HIPAA policies and procedures to address the changes made by ARRA. In addition, they will need to train their employees on these important changes. The contracts between business associates and covered entities will need to be updated and amended to reflect ARRA's changes. Health Information Exchange Organizations, Regional Health Information Organizations, E-prescribing Gateways, and other organizations not previously included within HIPAA's definition of "business associate" will have to enter into business associate agreements for the first time with covered entities.

Covered entities will need to revise their HIPAA privacy notice to incorporate changes to an individual's right to request a restriction on the disclosure of some PHI. Covered entities will need to review their liability insurance contracts and make changes to ensure that they are covered for potential HIPAA violations given the increased requirements and penalties. Covered entities also will need to develop and institute new breach notification procedures that comply with ARRA's federal breach notification requirements. They will need to work with a team of information security specialists to adopt new and potentially very costly technologies such as encryption or data destruction methods to ensure that all PHI they handle is considered "secure" and, thus, not subject to the breach notification requirements.

Finally, covered entities will need to develop a new accounting method to track disclosures of PHI to comply with the increased rights of individuals to know when their PHI has been disclosed. While these changes will burden covered entities because they will be expensive and disruptive to implement, the benefits outweigh the burdens. Congress should be commended for using the stimulus bill as an opportunity to improve the health of all Americans by investing in health information technology that will result in fewer medical errors and efficient health care delivery while simultaneously taking broad sweeping steps to ensure greater protection of personal health information.

Corrine P. Parver, Esq., is a Practitioner-in-Residence and Executive Director of the Health Law Project, Program on Law and Government, American University Washington College of Law. A member of the Health Care Compliance Editorial Advisory Board, Parver is a retired partner of Dickstein Shapiro LLP, where she headed the firm's Health Law Services Practice.

Savannah Thompson-Hoffman is a second-year law student at American University Washington College of Law.

1 American Recovery and Reinvestment Act of 2009 (ARRA)(PubLNo 111-5).
2 HIPAA (PubLNo 104-191).
3 45 C.F.R. §164.310.
4 45 C.F.R. §164.312.
5 45 C.F.R. §164.308.
6 *Supra* n. 1 at §13401(a).
7 45 C.F.R. §164.504(e).
8 45 C.F.R. §160.103.
9 45 C.F.R. §160.103(i)(A).
10 45 C.F.R. §160.103(ii).
11 *Supra* n. 8.
12 Center for Democracy and Technology, Policy Post 15.2: *Improvements and Challenges in Health Privacy Law*, http://www.cdt.org/publications/policyposts/2009/2, March 27, 2009.
13 *Supra* n. 1 at §13408.
14 *Id.* at §13408.
15 *Id.* at §13400(1)(A).
16 *Id.* at §13400(1)(B)(i).
17 *Id.* at §13400(1)(B)(ii).
18 *Id.*
19 *Id.* at §13402(c).
20 *Id.* at §13402(d)(1).
21 *Id.* at §13402(e)(1)(A).
22 *Id.* at §13402(e)(1)(B).
23 *Id.* at §13402(e)(3).
24 *Id.* at §13402(e)(2).
25 *Id.* at §13402(f).
26 *Id.* at §13407(a).
27 *Id.* at §13402(h)(1)(B).
28 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable, Final rule, 74 FR 19006, 19009 (April 27, 2009) (to be codified at 45 C.F.R. parts. 160, 164).
29 *Id.* at 19008.
30 *Id.*
31 *Supra* n. 1 at §13405(a).
32 Office for Civil Rights, *OCR Privacy Brief: Summary of the HIPAA Privacy Rule*, May 3, 2009.
33 *Supra* n. 1 at §13405(c)(1)(B).
34 Center for Democracy and Technology, Policy Post 15.2: *Improvements and Challenges in Health Privacy Law*, http://www.cdt.org/publications/policyposts/2009/2, March 27, 2009.
35 *Supra* n. 1 at §13410(c).
36 Majority Staff of the Committees on Energy and Commerce, *Ways and Means, and Science and Technology, Title IV - Health Information Technology for Economic and Clinical Health Act*, Jan. 16, 2009.
37 *Id.* at 21.
38 *Supra* n. 1 at §13406(b).
39 C. Stephen Redhead, *CRS Report for Congress: The Health Information Technology for Economic and Clinical Health (HITECH) Act*, at 22, Feb. 23, 2009.
40 *Supra* n. 1 at §13410(d)(3).
41 *Id.* at §13410(d)(1)(A).
42 *Id.*
43 *Id.* at §13410(e).
44 *Id.* at §13401.
45 *Id.* at §13403(a).
46 *Id.* at §13403(b).