

Bloomberg

**LAW
REPORTS[®]**
Privacy & Information

VOL. 2, NO. 4

April 2009

BLOOMBERG LAW REPORTS®

Privacy & Information

a
BLOOMBERG LAW™
publication

BLOOMBERG LAW REPORTS®—Privacy & Information is one in the comprehensive set of analytical reports from BLOOMBERG LAW™. For more information about BLOOMBERG LAW™ or the BLOOMBERG PROFESSIONAL® service, call:

In the US +1 212 617 6569

In EMEA +44 20 7330 7500

In Asia +852 2977 6407

Featured Article

Health Care Privacy and Security Law Reform in the American Recovery and Reinvestment Act: Sweeping Changes for the Health Care Sector

*Contributed by Linda A. Malek and Jay D. Meisel,
Moses & Singer LLP*

The historically slow adoption of electronic health records and personal health records by health care providers and individuals¹ just received a shot in the arm with \$19 billion in stimulus money authorized by the recently enacted American Recovery and Reinvestment Act (“ARRA”) to boost the implementation of health information technology. But will this “medicine” prove to be too much for a health care sector that already feels overburdened by privacy and security regulation? Lawmakers used this infusion of federal dollars into the health care sector as an opportunity to also make reforms to health care privacy and security law that privacy advocates had championed over the past few years. Given the expectation of expanded use of electronic and personal health records emanating from the spending authorized by ARRA, Congress and the Obama Administration included provisions in ARRA to make federal law more responsive to the challenges that the expanded use of electronic and personal health records will undoubtedly present.²

ARRA includes health information breach notification provisions and substantial changes to the Health Insurance Portability and Accountability Act (HIPAA). Privacy advocates view these changes as necessary to bring federal privacy and security law up to speed with recent developments in health care technology. Many providers, insurers and other businesses involved in the health care sector believe that these changes will result in the addition of unnecessary layers of complexity and regulation to their infrastructure and personnel administration. Both sides have valid arguments. An individual's health information should not be vulnerable in an era when the electronic transmission of sensitive information is susceptible to various security threats. However, in practice, some aspects of ARRA's health care privacy and security reform may prove to be quite burdensome, as the costs of certain provisions of the legislation may be significant.

This article will discuss the new provisions in federal law that increase privacy and security protections, such as those that require notification in the event of a breach of unsecured health information and that amend HIPAA with respect to business associates, covered entities that use electronic health records, marketing, stepped-up enforcement and other aspects of the HIPAA Privacy and Security Rules. It will also examine some

of the tensions and burdens these new provisions may create. This article will recommend steps to take for entities affected by the new breach notification and HIPAA provisions in order to comply with changes to the law.

Security Breach Notification

ARRA mandates that a HIPAA covered entity that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured protected health information” which discovers a breach of such information must notify each individual directly affected by such breach.³ Unsecured protected health information, according to ARRA, means protected health information that is not secured through a technology or methodology that the Department of Health and Human Services (HHS) has stated renders the protected health information unusable, unreadable or indecipherable to unauthorized individuals.⁴ HHS must issue guidance within 60 days after the enactment of ARRA that identifies technologies and methodologies satisfying this requirement.⁵ This guidance should inform covered entities as to the adequacy of their existing security infrastructures with respect to securing protected health information and whether changes need to be made to such infrastructures.

The notification to individuals must include, among other things: (1) the description and, if known, date of the breach; (2) steps an individual should take to protect against harm which may result from the breach and (3) a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.⁶ The new law also requires that business associates of HIPAA covered entities notify affected covered entities following the discovery of a breach by the business associate, and include in the notification the identification of each affected individual.⁷

ARRA also imposes notification requirements on vendors of personal health records, such as Google or Microsoft, and other non-HIPAA covered entities, such as a third party service provider that provides software support services. Specifically, any such vendors that discover a breach in security of an unsecured personal health record that is a personal health record maintained or offered by such vendor or entity must notify each individual who is a citizen or resident of the United States and whose unsecured personal health record information was acquired by an unauthorized person as a result of such a breach in security.⁸ The notification must include the same elements as described above for HIPAA-covered entities.⁹ This is an important addition to federal privacy law, since, in the past, there were no regulations governing personal health record vendors which were not covered entities or business associates.

The new law also requires that after a breach occurs which affects more than five hundred individuals, a HIPAA covered entity must notify HHS and prominent media outlets.¹⁰ In turn, HHS will post on its website a list that identifies each covered entity involved in a particular breach.¹¹ With respect to vendors of personal health records and other non-HIPAA covered entities, these vendors or entities must notify the Federal Trade Commission in the event of a security breach of health records.¹²

HIPAA-covered entities and vendors of personal health records have sixty days from the discovery of a breach to notify affected individuals. Business associates of HIPAA covered entities and other non-HIPAA covered entities have sixty days from the discovery of the breach to notify the appropriate covered entity or personal health record vendor.¹³

HHS must promulgate interim final regulations no later than 180 days after the enactment date of ARRA. The breach notification provisions shall become effective 30 days after such regulations are published.¹⁴

While over forty-five states currently have security breach notification laws, few include notification obligations specific to situations in which health information is compromised.¹⁵ Usually, security breach notification laws focus only on breaches of personal identification and financial information. However, ARRA broadens the scope of notification obligations for any entity dealing with health information either covered by HIPAA, in electronic format or both. In some cases, a breach of even *paper* records that contain unsecured protected health information may trigger notification requirements. Also, the sixty day notification period is a departure from most state security breach regulations that generally require notification only within a reasonable amount of time.¹⁶ ARRA preempts state law in the same way HIPAA does; generally ARRA supersedes any contrary state law, so if a state breach notification provision runs contrary to ARRA, it is now void.¹⁷ However, a state law that is more stringent with respect to security breach notification obligations should still remain effective.

In some ways, the security breach notification provisions are not a significant departure from existing state security breach notification provisions. The threshold for notification of a breach and the elements a notification must contain are similar to already promulgated state regulations, so businesses dealing with health information that have adequate security infrastructures and policies in place may only need to update their existing business practices. Businesses would only need to ensure that the security of health information, along with basic personal and financial information, is now included as an element of their breach notification policies. Still, the notification provisions are viewed as problematic

by some in the health care industry. For instance, John Houston, Vice President of Information Security and Privacy at the University of Pittsburgh Medical Center testified at a January 2009 Senate Judiciary Committee hearing that he had “serious concerns about the privacy components of [ARRA].”¹⁸ He said that, for example, he was concerned “that there will be a limited practical benefit associated with the web site posting or media notice [requirement], in relation to the associated effort...Further, it would appear that the purpose of reporting breaches is punitive, rather than serving a constructive purpose.”¹⁹ Another concern with the security breach notification provisions is that, because HHS has not yet issued guidance or final regulations as to how an entity must secure health information to comply with ARRA, it is too soon to determine whether the law will add undue complexity and costs to health care entities’ storage, maintenance and provision of individuals’ health information.

Changes to HIPAA

ARRA makes the most significant changes to federal health care privacy law since the promulgation of the Administrative Simplification provisions of HIPAA in statute in 1996 and the complementary privacy and security regulations enacted in 2000. It amends the HIPAA Privacy and Security Rules, affecting both HIPAA-covered entities and business associates.

Starting in February 2010, ARRA will subject business associates to many of the health information protection obligations that the Privacy and Security Rules currently mandate for covered entities and will require that any vendors that contract with covered entities to offer personal health records to individuals must have business associate agreements with such covered entities. For example, business associates will be required to implement the technical, physical and administrative safeguards of the Security Rule. Business associates will also be limited to using and disclosing protected health information only as allowed by the Privacy Rule.²⁰ They will be directly subject to civil and criminal penalties should they violate such security provisions, as opposed to the current standard whereby liability under HIPAA only extends to business associates by virtue of their business associate agreements with covered entities.²¹ Furthermore, ARRA stipulates that a business associate, in the event a covered entity fails to cure a material breach under its business associate agreement, must terminate such business associate agreement, or, if termination is infeasible, notify HHS of the uncured breach.²² Finally, any new requirements imposed on business associates by ARRA must be incorporated into business associate agreements by February 2010.²³

With respect to HIPAA's "minimum necessary" standard (i.e. a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request), a covered entity, under ARRA, must limit the use, disclosure, or request of protected health information to a limited data set to the extent practicable.²⁴ A limited data set consists of protected health information from which an extensive list of personal identifiers is removed.²⁵ In the past, the use of limited data sets were contemplated only in situations where clinical research or public health activities were conducted; limited data sets were not linked to compliance with the minimum necessary rule. With these changes, covered entities will need to make use of limited data sets more frequently when disclosing health records, and this will inevitably increase their administrative burden. This provision is a clear victory for privacy advocates as it adds more restrictive limitations to the disclosure of protected health information. However, one could argue that it provides needed clarity to the minimum necessary rule from which providers and other covered entities will eventually benefit as well.

For entities that use or maintain electronic health records, ARRA eliminates the exception under the HIPAA Privacy Rule that allows covered entities to exclude from their accounting to individuals disclosures of protected health information related to treatment, payment and health care operations.²⁶ This effectively means that a health care provider, insurer or any other covered entity using electronic health records will be subject to much more extensive reporting requirements, as disclosures related to treatment, payment and health care operations arguably make up the bulk of disclosures made by covered entities. ARRA also places a substantial new burden on certain business associates with respect to accounting for disclosures. It gives a covered entity the option to either directly account for disclosures of business associates acting on its behalf or to provide a list of business associates to be contacted by the individual requesting an accounting so that the business associate must report its own disclosures of protected health information.²⁷

In addition to the Privacy Rule's already existing provisions as to when an authorization is required for disclosures of protected health information, ARRA generally prohibits the sale of protected health information in certain instances unless a covered entity obtains a valid authorization that includes "a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information."²⁸

Also significant are the changes that ARRA makes to current practices regarding marketing under the HIPAA Privacy Rule. Specifically, the new law narrows restrictions on use

of protected health information for marketing purposes.²⁹ Current exceptions to HIPAA marketing rule, such as the one permitting communications encouraging purchase or use of products or services in connection with treatment or case management/care coordination are not allowed under the amendments that ARRA makes to the Privacy Rule if a covered entity is paid to make the communication unless (1) the marketing communication merely describes a currently prescribed drug or biologic for an individual and payment for such communication is reasonable in amount; (2) a covered entity obtains a written authorization from an individual; or (3) a business associate makes the communication consistent with the business associate agreement between it and a covered entity.³⁰ This revision to the Privacy Rule could be characterized as potentially overbroad, as it could inadvertently limit the paid promotion of preventive healthcare measures that are intended to result in a public benefit as well as restricting marketing communications which are simply designed to promote a particular product to maximize profits.

ARRA enhances penalties for non-compliance with HIPAA by increasing civil monetary penalties, as it correlates such fines to the level of a particular violator's intent.³¹ It also strengthens HIPAA enforcement mechanisms by authorizing state attorneys general to enforce violations of the HIPAA privacy and security rules against covered entities as well as business associates under certain circumstances.³² Privacy advocates welcome this change, as Ashley Katz, executive director of the group Patient Privacy Rights, points out that federal enforcement of HIPAA has been "virtually non-existent", with the notable exception of the recent Federal Trade Commission action against CVS Caremark Corp.³³ However, industry representatives such as Patty Goldman of the American Hospital Association are not enthusiastic about the increased enforcement measures. Goldman stated that "We don't need 51 more interpretations" of the legal and regulatory requirements of the HIPAA privacy rules which now are subject to federal enforcement."³⁴

The Impact on Health Care Entities and Other Businesses Involved with Health Records

The substantial changes to HIPAA and the new regulation of electronic health records signals a marked shift by the federal government to control the flow of health information as it prepares to make unprecedented amounts of money available for health information technology initiatives. While they are potentially burdensome, they will ultimately regulate a more robust health care information technology sector. The day-to-day costs of administering a more highly regulated health information technology environment may increase, but, in the long run, we can hope that, as President Obama said in an address in January 2009, computerizing America's medical

records “won’t just save billions of dollars and thousands of jobs – it will save lives by reducing the deadly but preventable medical errors that pervade our healthcare system.”³⁵

To prepare for the changes in the law described above, and for more detailed regulations that HHS will promulgate in the near future, health care entities and other entities that are business associates and/or deal with electronic and personal health records should review their existing privacy policies and procedures and update them to reflect the new requirements with respect to HIPAA, security breach notification, and other relevant aspects of ARRA. Covered entities in particular should review and modify their business associate agreements to comply with the new obligations for business associates. Non-covered entities that are business associates face greatly increased compliance obligations and will need to implement administrative, technical and physical safeguards by developing policies and procedures, as business associates now face direct liability for non-compliance with certain provisions of HIPAA, as discussed previously. Non-compliance with federal privacy law can now result in even larger civil monetary penalties. Lastly, and of great significance, is the fact that with the increased risk of public exposure resulting from ARRA’s security breach notification requirements, companies doing business in the healthcare sector should take all measures necessary to ensure that protected health information is held securely to guard against unauthorized access.

Linda A. Malek is a partner at Moses & Singer LLP, chair of the firm’s Healthcare practice group and co-chair of the firm’s Privacy practice group. Jay D. Meisel is an associate in the firm’s Healthcare and Privacy practice groups. Moses & Singer counsels a variety of entities in the healthcare industry and other industry sectors on matters related to privacy and security. For more information on this topic, please contact Linda A. Malek at lmalek@mosessinger.com or 212-554-7814 or Jay D. Meisel at jmeisel@mosessinger.com or 212-554-7823. For further information about Moses & Singer LLP, please visit www.mosessinger.com.

¹² *Id.*

¹³ *Id.* at 13407.

¹⁴ *Id.* at 13402.

¹⁵ California and Arkansas are notable exceptions; each has security breach notification requirements with respect to “medical information” and California also includes “insurance information.”

¹⁶ For example, New York’s security breach notification law states: “The disclosure shall be made in the most expedient time possible and without unreasonable delay.”

¹⁷ American Recovery and Reinvestment Act of 2009 at §13421.

¹⁸ *Health IT: Protecting Americans’ Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 111th Cong (2009) (statement of John Houston, Vice President of Information Security and Privacy University of Pittsburgh Medical Center).

¹⁹ *Id.*

²⁰ American Recovery and Reinvestment Act of 2009 at §§ 13401 and 13404.

²¹ *Id.*

²² *Id.* at 13404.

²³ *Id.* at §§ 13401 and 13404.

²⁴ *Id.* at § 13405.

²⁵ 45 CFR Part 164.514(e)(11)

²⁶ American Recovery and Reinvestment Act of 2009 at § 13405.

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.* at 13406.

³⁰ *Id.*

³¹ American Recovery and Reinvestment Act of 2009 at § 13410.

³² *Id.*

³³ *Stakeholders Disagree on Whether Stimulus Breach Notice is Positive*. BNA Privacy & Security Law Report, March 2, 2009, at 329.

³⁴ *Id.*

³⁵ President-elect Barack Obama, Address at George Mason University (January 8, 2009).

¹ See e.g. American Hospital Association. “Continued Progress: Hospital Use of Information Technology” (2007) at 3. (In late 2006, approximately 11 percent of hospitals had a fully implemented EHR system).

² As defined in ARRA, an electronic health record is an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. A personal health record is an electronic record of individually identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or for the individual. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13400.

³ *Id.* at § 13402.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ *Id.* at 13407

⁹ *Id.*

¹⁰ *Id.* at 13402.

¹¹ *Id.*

MOSES & SINGER LLP

Disclaimer

Viewing this document or contacting Moses & Singer LLP does not create an attorney-client relationship.

This document is intended as a general comment on certain recent developments in the law. It does not contain a complete legal analysis or constitute an opinion of Moses & Singer LLP or any member of the firm on the legal issues herein described. This document contains timely information that may eventually be modified or rendered incorrect by future legislative or judicial developments. It is recommended that readers not rely on this general guide in structuring or analyzing individual transactions or matters but that professional advice be sought in connection with any such transaction or matter.

Attorney Advertising

It is possible that under the laws, rules or regulations of certain jurisdictions, this document may be construed as an advertisement or solicitation.