

Client Alert: Stimulus Bill Makes Sweeping Changes to Federal Health Care Privacy Laws

On February 17, 2009 the American Recovery and Reinvestment Act (“ARRA”) was signed into law by President Obama, bringing major changes to the health care sector. Not only does ARRA contain \$789 billion in spending provisions, it also includes sweeping changes to health information privacy law. Given the provisions in ARRA that authorize spending billions of dollars to boost the implementation of health information technology, lawmakers felt it was necessary to make federal law more responsive to the challenges that the expanded use of electronic and personal health records will undoubtedly present.¹ Most notably, ARRA includes health information breach notification provisions and substantial changes to the Health Insurance Portability and Accountability Act (HIPAA).

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. 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. HHS must issue guidance within 60 days after the enactment of ARRA that identifies technologies and methodologies satisfying this requirement. 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. 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.

ARRA requires that vendors of personal health records and other non-HIPAA covered entities, such as a third party service provider that provides software support services, 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. The notification must include the same elements as described above for HIPAA-covered entities.

¹ 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.

The new law also requires that after a breach occurs which impacts more than five hundred individuals, a HIPAA covered entity must notify the HHS and prominent media outlets. In turn, HHS will post on its website a list that identifies each covered entity involved in a particular breach. 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.

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.

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.

While over forty-five states currently have security breach notification laws, few include notification obligations if health information is compromised. 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. 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. However, a state law that is more stringent with respect to security breach notification obligations should still remain effective.

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. 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. 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. Finally, any new requirements imposed on business associates by ARRA must be incorporated into business associate agreements by February 2010.

ARRA requires that, in order for a covered entity to be compliant with the “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) with respect to the use, disclosure, or request of protected health information, a covered entity must limit such protected health information to a limited data set to the extent practicable. A limited data set consists of protected health information from which an extensive list of personal identifiers is removed. In the past, the use of limited data sets were typically required in situations where clinical research or public health activities were conducted; limited data sets were not linked to compliance with the minimum necessary rule.

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. 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.

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.”

Also, significant are the changes that ARRA makes to current practices regarding marketing under the Privacy Rule. Specifically, the new law narrows restrictions on use of protected health information for marketing purposes. Current exceptions to the 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.

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. 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.

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.

Health care entities and other businesses that deal with personal and/or electronic health records should view these changes to the law with cautious optimism. While they are potentially burdensome, they will ultimately regulate a more robust health care information technology sector.

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. Also 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 and serious breaches with respect to protected health information can irredeemably damage the reputation of a company doing business in the health care sector.

If you have any questions regarding this Client Alert, please contact:

Linda A. Malek
(212) 554-7814
lmalek@mosessinger.com

Cathy J. Frankel
(212) 554-7848
cfrankel@mosessinger.com

Jeffrey M. Davis
(212) 554-7837
jdavis@mosessinger.com

David Rabinowitz
(212) 554-7815
drabinowitz@mosessinger.com

Abraham (Avi) Y. Skoff
(212) 554-7897
askoff@mosessinger.com

Jill E. Anderson
(212) 554-7836
janderson@mosessinger.com

Jay D. Meisel
(212) 554-7823
jmeisel@mosessinger.com

Samuel J. Servello
(212) 554-7872
sservello@mosessinger.com

MOSES & SINGER LLP

Moses & Singer LLP has served its clients skillfully and decisively since 1919. We provide cost-effective and result-focused legal services in the following primary areas:

- Banking and Finance
- Business Reorganization, Bankruptcy and Creditors' Rights
- Corporate Securities and M & A
- Employment and Labor
- Entertainment, Advertising, IP and Internet/Technology
- Healthcare
- Hotel and Hospitality

- Litigation
- Matrimonial
- Private Funds
- Legal Ethics & Law Firm Practice
- Real Estate
- Tax
- Trusts and Estates and Wealth Preservation

The Chrysler Building
405 Lexington Avenue
New York, NY 10174-1299
Tel: 212.554.7800
Fax: 212.554.7700

2200 Fletcher Avenue
Fort Lee, NJ 07024
Tel: 201.363.1210 Fax: 201.363.9210
Abraham Y. Skoff, Esq.,
Managing Attorney for New Jersey

Disclaimer

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

To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

Attorney Advertising

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

Copyright © 2009 Moses & Singer LLP
All Rights Reserved