

[Home](#)[Register](#)

Massachusetts Backs Off Again on Information Security, While the Feder Stimulus Bill Rams Through Much More Stringent Standards

-- By Jon Neiditz, Cindy Hutto, Amanda Witt and Eli Poliakoff of [Nelson Mullins](#)

If you are trying to recover from that case of whiplash from trying to keep up with legis regulatory trends in this economic downturn; do not turn your attention to the area of i security. Massachusetts just delayed implementation of its stringent information securit again, purportedly due to the economic downturn, just as the federal American Recover Reinvestment Act of 2009 imposed massive new information security burdens on all par the healthcare economy in response, of course, to the economic downturn. One imagine bewigged gentlepeople of Massachusetts pausing in their debate on the niceties of their security rules to turn their eyes upward from their cobblestone streets and watch the G federal stimulus package consume the entire issue for a large chunk of the US economy

1. Massachusetts Backs Off...

Massachusetts just keeps backing off from the effective dates and some of the require information security standards to get more buy-in from the business community, but m. achieve that goal even now. The initial effective date of its information security regulati CMR 17.00) was pushed back some months ago by the Office of Consumer Affairs and E Regulation from January 1, 2009 to May 1, 2009 for most of the regulations. Now, as ar the Office on February 12, 2009, businesses that hold personal information of Massachu residents (namely, a combination of a name along with a Social Security number, credit number or bank account number) will have until January 1, 2010 before they must com new regulations that require, among other things, the encryption of wireless transmissic personal information and the encryption of personal information stored on portable devi personal information such as laptops, flash drives and PDAs.

Besides delaying the effective date, the Massachusetts information security regulations revised to remove the requirements that third party service providers with access to pei information certify in writing that they have a written information security program that with the Massachusetts regulations and contractually commit to maintain those standar revisions also modify in ways that are proving confusing the former requirement that a take reasonably steps to ensure that its third party service providers be capable of mair those safeguards for personal information. Now such third party service providers must capacity to protect personal information in accordance with the Massachusetts regulatio owner of the personal information must take "all" reasonable steps to ensure that such service provider is applying safeguards at least as stringent as those imposed by the rul spokesperson for the Commonwealth indicates that the change was designed to make tl more flexible for businesses of different sizes and risk profiles, but many believe that th not see it that way.

Lastly, it appears that the regulations were corrected by limiting the requirement to enc transmitted wirelessly to requiring encryption of such data only if it contains personal in defined by the regulations. Even with the revisions, it will likely be very difficult for sma to fully comply with these highly detailed and demanding regulations.

Please review our earlier article on the initial release of the Massachusetts regulations [h](#) information on its requirements.

2. ...As the Feds Barrel In: Information Security and HIPAA Provisions of the Recovery and Reinvestment Act of 2009

As it did with the promulgation of rules under the "Administrative Simplification" provisions of HIPAA, the desire to save administrative costs in health care through electronic process resulted in major new information security and privacy protections in the American Recovery and Reinvestment Act of 2009 ("ARRA").

Regulation of Business Associates

A very wide-ranging impact of ARRA in the information security area is in its application to business associates of core requirements of HIPAA's Security Rule - technical, administrative, physical safeguards and policies and documentation requirements - that previously applied only to covered health care providers, health plans and clearinghouses. This provision effectively extends specific HIPAA security requirements - rather than the vague requirements that until now applied only to business associates - throughout the healthcare economy. Moreover, the impact of this may be greatly magnified by a requirement that the Secretary of DHHS issue annual guidance on technical safeguards.

The requirements for covered entities under HIPAA's Privacy Rule, on the other hand, are not applicable to business associates. However, both the privacy and security requirements detailed below are made applicable to business associates as well as covered entities, and business associate agreements are required to be modified to include all such requirements. We have begun to see jokes about whether the requirement to contract for provisions that apply to business associates is viewed as economic stimulus; in any case, it is indeed worth remembering that the reason for the creation of business associates and business associate agreements was to extend the jurisdiction of the HIPAA Administrative Simplification provisions to the three types of covered entities, and the consequent need to reach the many participants in health care that the HIPAA rules could not reach through requirements placed on covered entities to contract with those participants. Now that ARRA extends statutory authority to cover all business associates, one can only hope for regulatory relief regarding an obligation to impose the same requirements by contract.

Application of HIPAA Enforcement Penalties to Business Associates

Of equally broad impact is expansion of civil and criminal penalties previously applicable only to covered entities to all business associates. Although the apparent intent of this expansion is to extend HIPAA enforcement to business associates to enforcement "in the same manner as" covered entities, the standards enforced will only be the same regarding security issues; with regard to privacy issues, civil and criminal enforcement penalties will apply to business associates as to covered entities, but the rules being so enforced for business associates will remain much broader and vague than the rules for covered entities.

Breach Notification Procedures for Business Associates and Covered Entities

ARRA requires a covered entity which discovers a breach of unsecured protected health information to notify each individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of the breach. A business associate must notify the covered entity upon discovery of a breach of unsecured protected health information.

The ways in which these provisions interact with the forty-five (45) state breach notification laws will no doubt receive a great deal of analysis in the coming months. It is important, however, to note that currently only six (6) of those state laws cover breaches involving only paper rather than electronic information, and all of them require notices only when a combination of elements is met to create a risk of identity theft - such as name, address and social security number - is

The remarkable effect of the choice of ARRA's drafters to make breaches of unsecured protected health information (which can be generally described as any information that identifies an individual and has been created or received by a covered entity) notice-triggering appears to make no sense in the context of breaches of paper-based information but breaches of information through the spoken word are potentially notice-triggering. Requiring breach notification when conversations inadvertently disclose individual-identifying information is, needless to say, a major departure from current law in the area of security breaches. As noted below, HIPAA's provisions related to the enforcement of state laws continue to apply. However, in practice it may be difficult to determine what

ARRA breach standards are "more stringent than" state laws because of the entirely different analysis prescribed in the new federal and all state provisions.

The notification provisions are limited by ARRA's definition of "breach," and "unsecured health information." "Breach" is the unauthorized acquisition, access, use, or disclosure of health information which compromises the security or privacy of such information. A breach does not include situations where a person would not reasonably be able to retain the information. A variety of unintentional acquisitions or disclosures generally limited to access within the entity or business associate. As such, certain disclosures of protected health information trigger notification requirements.

Similarly, the notification provisions apply only to "unsecured" protected health information as information that is not secured through the use of a technology or methodology as specified by the Secretary. Within 60 days after enactment of ARRA the Secretary is to issue guidance regarding technologies and methodologies that render information "secured." If the Secretary does not issue guidance within that timeframe, the acceptable standards will include those that render health information unusable, unreadable, or indecipherable to unauthorized individuals: developed or endorsed by a standards developing organization that is accredited by the National Standards Institute.

Notice of the breach must be made within 60 days of discovery and provided by mail, e-mail (if specified as preference by the individual), phone (if imminent misuse expected) and/or websites or in the media (in cases of insufficient contact information). Notice must also be provided to the Secretary and "prominent" media outlets serving a particular area if more than 500 individuals in that area were impacted. Breaches affecting less than 500 individuals must be reported in a log that is submitted annually to the Secretary. Notably, the covered entity or business associate has the burden of demonstrating that all required notifications were made, including evidence demonstrating the necessity of any delay. Additionally, the notice is not delayed if a law enforcement official determines that the notice would impede a criminal investigation.

The Secretary is to issue interim final regulations within 180 days of the enactment of ARRA. Breach notification requirements will apply to breaches that are discovered on or after 30 days following the publication of the interim final regulations. Therefore, these breach notification requirements will be effective no later than September 15, 2009 (approximately 210 days after February 17, 2009).

"Minimum Necessary" Provisions

The Bill adds that a covered entity may be treated as meeting the "minimum necessary" standard by limiting the protected health information to the limited data set as defined by HIPAA, as long as the covered entity or business associate disclosing the protected health information to the recipient - determines what constitutes the minimum necessary to meet existing HIPAA requirements. The Secretary must issue guidance as to what constitutes "minimum necessary" purposes of the HIPAA Privacy Rule no later than 18 months after the enactment of the provisions in the Bill identifying "minimum necessary" will sunset on the effective date of the Secretary's Guidance. Covered entities, therefore, will be required to engage in additional analysis once the guidance is issued to ensure they remain in compliance with the "minimum necessary" standard.

Accounting of Disclosures of Electronic Health Records

Under current law, an individual can receive an accounting of protected health information by a covered entity over the last six years, except for disclosures made to carry out treatment, payment and health care operations. ARRA removes this exception for disclosures through an electronic health record and provides that an individual may receive an accounting of disclosures through an electronic health record for the prior three years. In addition to addressing disclosures, covered entities must either provide an accounting of disclosures made by the entity or identify the business associate, who must respond to direct requests when made by an individual. Additional regulations will be issued on the method of tracking such disclosures. Covered entities that acquire electronic health records after January 1, 2009, these accounting provisions are effective the later of January 1, 2011; the date it acquires an electronic health record or a later date set by the Secretary (but no later than 2013).

Limitations on Sale of Electronic Health Records or Protected Health Information

ARRA prohibits a covered entity or business associate from directly or indirectly receiving remuneration in exchange for any protected health information unless the individual to whom the information relates consents or an exception applies. The exceptions include, but are not limited to, public health activities, research, the individual's treatment or health care operations, or other activities otherwise addressed in regulations to be issued by the Secretary within 18 months of the date of enactment of ARRA. These limitations apply to exchanges occurring on or after 6 months following the date of the final regulations.

Access to Information in Electronic Format

Existing HIPAA provisions permit individuals to obtain a copy of certain protected health information. ARRA amends this provision to permit individuals to obtain the information in electronic format. ARRA limits the fees imposed for providing the information to the labor costs incurred in responding to the request.

Limitations on disclosure pursuant to "Health Care Operations"

The Bill clarifies the existing HIPAA provisions that permit disclosure of protected health information for "health care operations" purposes, as defined by the HIPAA Privacy Rule, and the prohibition on disclosing protected health information for marketing purposes without authorization. The Bill clarifies that certain marketing communications by a covered entity or business associate for a service or product that encourages the recipient to purchase or use the service shall not be considered "health care operations" unless it generally relates to a health-care related product or service and certain other requirements are met.

Specifically, a covered entity cannot receive direct or indirect payment for making such a communication unless the payment is "reasonable in amount." The term "reasonable in amount" will be defined by the Secretary in regulation. The communication must also pertain to a service or product currently prescribed to the recipient to be considered "health care operations" if it is a "marketing" communication.

In the alternative, the covered entity may obtain an authorization from the recipient of the communication consistent with the current HIPAA authorization requirements. Finally, the communication may be made by a business associate consistent with the business associate agreement. Given that a business associate is not permitted to do anything under the HIPAA Privacy Rule that a covered entity is not permitted to do, any communications by a business associate under this section would be subject to the same limitations as a covered entity under the section above. These requirements take effect 12 months after enactment of the Bill.

Examples of communications that appear to be subject to the new limitations include sending information to current patients on generic alternatives or new drug treatments because the alternatives would not be currently prescribed to the recipient. Other examples include recommending alternative treatments or therapies if the covered entity receives payment for the communication. The covered entity could, however, obtain an authorization to permit such communications. It will be important to continue to monitor this area as the new regulations and any additional regulations issued by the Secretary.

Fundraising Communications

ARRA continues to permit fundraising activities by the provider using a patient's protected health information so long as any written fundraising materials provide an opportunity to opt out of fundraising communications. If the recipient chooses to opt out of future fundraising communications, that choice is treated as a revocation of authorization under existing provisions of the HIPAA Privacy Rule that guarantee rights for individuals who revoke such authorization, including the right not to be denied treatment as a result of making that choice. These provisions take effect 12 months after enactment.

Breach Notification Procedures for Vendors and Service Providers

For those vendors of personal health records that are not also business associates, ARRA parallel breach notification requirements. Generally, notice must be provided to individuals following the discovery of a security breach of information that is provided by, or to the individual and can reasonably identify the individual. "Vendors" is defined as any entity other than a covered entity, that offers or maintains a personal health record. Similar notification requirements are imposed on third party service providers that provide service to vendors of personal health information. Similar to the breach notification provisions for covered entities and business associates, the requirements on vendors and service providers apply only to the disclosure of personal health information. The method, content and time requirements for such notifications are also those imposed on business associates and service providers. Notably, a violation of the requirements under this section is considered an unfair or deceptive practice under the Federal Trade Commission Act.

The Federal Trade Commission ("FTC") must issue interim final regulations for such notifications within 180 days of the enactment of ARRA. The breach notification requirements will apply to breaches that are discovered on or after 30 days following the publication of the interim regulations. Therefore, these breach notification requirements will be effective no later than September 15, 2009 (approximately 210 days following February 17, 2009). These regulations sunset if Congress enacts new legislation for notification that applies to entities that are not covered entities or business associates.

Business Associate Contracts for Health Information Exchanges

ARRA requires organizations that contract with covered entities or their business associates for the purpose of exchanging electronic health information, such as Health Information Exchanges, Regional Health Information Organizations, and PHR vendors that offer their products through a provider or health plan, to have business associate contracts with those providers or health plans. Similarly, such entities are to be treated as business associates, thus imposing the breach notification provisions and other requirements.

Criminal Penalties for Employees and Other Individuals

ARRA clarifies that criminal penalties for wrongful disclosure of PHI apply to individuals who are not authorized to obtain or disclose such information maintained by a covered entity, whether they are employees or not. The amendment reverses prior legal direction by the Justice Department.

Enhanced Enforcement and Civil Penalties

ARRA significantly enhances the government's enforcement capabilities and penalties.

ARRA amends HIPAA to permit the Office of Civil Rights ("OCR") to pursue an investigation and imposition of civil monetary penalties against any individual for an alleged criminal violation of the HIPAA Privacy and Security Rule if the Justice Department had not prosecuted the individual. In addition, the bill amends HIPAA to require a formal investigation of complaints and the imposition of civil monetary penalties for violations due to willful neglect (existing law requires a high threshold). The Secretary is required to issue regulations within 18 months to implement the amendments, which shall apply to penalties imposed on or after 24 months following the date of enactment. Notably, the civil penalties collected are to be transferred to OCR for use in enforcing HIPAA privacy and security standards.

Additionally, within 18 months of enactment, the General Accounting Office ("GAO") must issue recommendations for giving a percentage of any civil monetary penalties collected to the harmed individuals. Based on those recommendations, the Secretary, within three years of enactment, must establish a methodology to distribute a percentage of any collected penalties to the harmed individuals.

ARRA also increases and tiers the penalties for HIPAA violations, effective upon the date of enactment.

Actions by State Attorneys General

Most significantly, and in a clear break from prior law, ARRA permits State Attorneys General

bring civil actions in federal district court against individuals who violate the HIPAA privacy security standards in order to enjoin further violations and obtain damages up to \$100,000 per violation, capped at \$25,000 annually, for all violations of an identical requirement or prohibition. The Secretary has discretion to award costs and reasonable attorneys' fees for successful actions. A suit is not permitted if a federal civil action is pending. This provision is effective upon enactment.

Periodic Audits

ARRA requires the Secretary to perform periodic audits of covered entities and business associates to ensure compliance with the Privacy and Security Rule promulgated pursuant to HIPAA requirements of this subtitle.

Relationship to Other Laws

The existing preemption principles of HIPAA apply to the requirements of ARRA. Where the ARRA is inconsistent with HIPAA, the Secretary will make HIPAA rules conform to ARRA. A puzzling construction note indicates that nothing in ARRA constitutes a waiver of "any protection otherwise applicable regarding protected health information, apparently encouraging care regarding the multitude of privileges that may be available.

Studies, Reports and Guidance

ARRA requires the Secretary to submit annually a number of reports, including but not limited to the number and nature of complaints of alleged violations and their resolution; civil fines imposed; the number of audits and summaries of the findings. The Secretary must also, in consultation with the FTC, study the application of health information privacy and security requirements on non-covered entities, including PHR vendors and related entities, and determine which federal agencies are best equipped to enforce new requirements for non-HIPAA covered entities.

Effective Date

Unless otherwise specified, the effective date of these provisions is 12 months following