

Health Care ADVISORY

March 3, 2009

American Recovery and Reinvestment Act of 2009: Privacy and Security Provisions “Up the Ante” for Covered Entities, Business Associates and Non-Covered HIPAA Entities

Overview

The American Recovery and Reinvestment Act of 2009 (ARRA or the “Act”)¹ was signed into law on February 17, 2009, by President Obama. The proposed economic stimulus bill was passed by Congress on February 13, 2009, amidst persistent negotiations between Democrats and pivotal Republican congressional members. ARRA includes several provisions impacting the health care industry, such as significant changes to the Privacy and Security Rules issued under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA Rules”). The Privacy Subtitle of ARRA sets forth provisions that drastically tighten the HIPAA law by making expansive changes to the privacy and security provisions impacting covered entities and business associates, and also entities not previously covered by the HIPAA Rules. Many of the provisions will be effective within a year of ARRA’s enactment and will be implemented through rulemaking as stipulated by the law.

Key Changes

ARRA incorporates a series of privacy and security provisions that will amplify the current requirements under the HIPAA Rules. Among other things, the legislation strengthens the enforcement of the HIPAA privacy and security standards, and establishes a notification requirement in the event of a security breach involving protected health information (PHI). Consequently, covered entities, business associates and other entities that use or maintain PHI risk the imposition of civil and criminal penalties for failure to comply. Further, these entities will incur significantly increased administrative costs and burdens in complying with the ARRA provisions.

This advisory highlights the key changes to the HIPAA Rules mandated by ARRA and the implications of these changes on covered entities and on non-covered entities, such as business associates and vendors. In addition, to illustrate these changes, a chart summarizing changes from existing law is included at the end of this advisory.

¹ The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009).

Application of Security and Privacy Provisions and Penalties to Business Associates

The HIPAA Security Rule permits business associates performing services for or on behalf of covered entities to create, access, receive, maintain or transmit PHI so long as the business associate agreement between the two entities meets certain requirements.² Similarly, the HIPAA Privacy Rule permits covered entities to disclose health information to a business associate or to allow a business associate to create or receive health information on a covered entity's behalf, so long as the covered entity is assured that such information will be protected in the manner outlined by the business associate agreement.³ Unlike covered entities, however, violations under the HIPAA Rules cannot be enforced by the government directly against business associates. Instead, although covered entities are not required to monitor the actions of their business associates, if a covered entity is made aware of a material breach or violation of the business associate agreement, the covered entity must make reasonable efforts to remedy the situation, terminate the agreement or, if terminating the contract is not feasible, report the issue to the Secretary of the Department of Health and Human Services (the "Secretary").⁴

Under ARRA, however, the HIPAA Rules relating to information security requirements for administrative, physical and technical safeguards of electronic PHI, as well as the privacy requirements set forth under HIPAA and ARRA, will apply directly to business associates in the same manner as those standards apply to covered entities. The civil and criminal penalties for violating the applicable privacy and security requirements of the HIPAA Rules and ARRA would also apply to business associates directly. Thus, business associates will be required to comply with most of the security requirements set forth in the HIPAA Rules, as if they were covered entities like health care providers. In addition, the Secretary, in consultation with stakeholders, will issue annual guidance on the most effective and appropriate technical safeguards for protecting electronic health information.

The full implications of this application to business associates will not be clear until the Secretary issues implementing regulations. However, the implication is that business associates will be required to meet a broad range of the requirements currently applicable to covered entities under the HIPAA Rules, such as obtaining patient authorization for certain uses and disclosures of PHI, establishing privacy and security policies and procedures, providing to patients rights of access, amendment and entitlement to an accounting of disclosures, conducting a security risk assessment for electronic PHI and many of the other extensive requirements of the HIPAA Rules.

² See 45 C.F.R. § 164.314.

³ See 45 C.F.R. § 164.502(e).

⁴ See 45 C.F.R. § 164.314(a)(1); see also 45 C.F.R. § 164.504(e)(1).

Notification of Breaches

Covered Entities and Business Associates

The HIPAA Rules currently do not require that covered entities notify individuals or the Secretary of a breach of the privacy, security or integrity of PHI. With respect to business associates, these entities are only required to include in their business associate agreements a provision requiring them to report to the covered entity the discovery of any security incident or any use or disclosure of PHI that is not addressed by their business associate agreement.⁵ ARRA, however, creates a new notification requirement for breaches of PHI that will have a significant impact on covered entities and business associates alike.

The Act provides that, in the case of a breach with respect to unsecured PHI,⁶ the covered entity would be required to notify each individual whose information has been, or is reasonably believed to have been, accessed, acquired or disclosed as a result of such a breach. If the breach of PHI involves a business associate, the business associate is required to notify the covered entity. ARRA defines the term “breach” as the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information. The definition, however, excludes certain inadvertent or unintentional disclosures, such as where one authorized user at a facility inadvertently discloses information to another authorized user at the same facility, so long as the information is not further acquired, accessed, used or disclosed without authorization. Thus, although the Act will broadly require that individuals be notified of breaches relating to their PHI, a covered entity would not necessarily be required to notify an individual each time there was an in-house breach of a patient’s PHI. Still, this notification requirement will impose a costly and burdensome new requirement on covered entities, particularly where a breach involves the PHI of a large number of individuals.

Beyond notifying the individual, which is to be done not later than 60 days after discovery of the breach, unless the notification would impede a criminal investigation or harm national security, covered entities also will be required to notify the Secretary of such breaches. If the breach involves 500 or more individuals, the notice to the Secretary must be immediate and the local media for the area where the individuals reside must also be notified. Where 500 or more individuals are involved, the Secretary is also required to post on the HHS Web site the list of covered entities involved in the breach. In the case of breaches involving fewer than 500 individuals, the covered entity may maintain a log and notify the Secretary of its breaches on an annual basis.

In implementing this requirement, the Secretary will promulgate interim final regulations within 180 days of the Act’s enactment. Further, 60 days after enactment, the Secretary (in consultation with stakeholders) will be responsible for annually putting forth guidance that will specify the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals (i.e., encryption).

⁵ See 45 C.F.R. § 164.314(a)(2); see also 45 C.F.R. § 164.504(e)(2).

⁶ ARRA defines the term “unsecured protected health information” as PHI that is not secured through the use of a technology or methodology specified by the Secretary as mandated by the Act.

The new notification requirement constitutes a very significant change from current law. Notifying all affected individuals of a breach can be very costly, and the requirements of notifying the Secretary and the media will have a significant negative public relations impact for covered entities. Because of these requirements, covered entities likely will be motivated to employ more extensive and expensive measures and technologies to safeguard PHI.

Entities Not Currently Covered Under the HIPAA Rules

Currently, there are no HIPAA provisions that require entities that are not covered entities or business associates to notify individuals when their health information has been breached. However, under ARRA, vendors of personal health records⁷ (PHRs) and other non-HIPAA-covered entities will be required to notify individuals of breaches. This requirement expands HIPAA far beyond the previous scope of the HIPAA Rules and demonstrates the new aggressive approach of Congress and the administration toward protecting PHI.

Specifically, the Act requires that PHR vendors and certain non-HIPAA-covered entities (e.g., entities offering products and services through a PHR vendor's Web site), upon discovering a breach of security of "unsecured PHR identifiable health information" that is in a PHR maintained or offered by such vendor or entity, to notify both the individuals affected by the breach and the Federal Trade Commission (FTC). The term "unsecured PHR identifiable health information" is PHR identifiable health information⁸ that is not protected through the use of a technology or methodology specified by the Secretary. In addition, third-party service providers that provide services to PHR vendors and to certain other non-covered entities (e.g., entities offering products and services through a PHR vendor's Web site) that handle unsecured PHR identifiable health information are required to notify the vendor or other entity. The timeliness and content requirements relating to such notifications that apply to covered entities and business associates also apply to these entities.

In carrying out this new requirement, the FTC is responsible for notifying the Secretary of any breaches. The enforcement authority for such breaches will be left with the FTC and any violations will be treated as unfair and deceptive acts or practices in violation of the Federal Trade Commission Act. The FTC is required to issue interim final regulations with respect to these provisions within 180 days of ARRA's enactment. Notably, the new privacy and security standards that apply under the Act to non-HIPAA-covered entities will be superseded by any new legislation enacted by Congress establishing breach notification requirements with respect to these entities.

⁷ ARRA defines the term "personal health record" as an electronic record of "PHR identifiable health information" on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.

⁸ The term "PHR identifiable health information" is defined as demographic information collected from an individual that either identifies the individual or can be used to identify the individual. See 42 U.S.C. § 1320d(6) (definition of "individually identifiable health information").

Patient Protections

At present, there are several individual privacy rights set forth by the HIPAA Privacy Rule. To illustrate only a few, first, the Privacy Rule established a new right for individuals to view and obtain copies of their own PHI in the form or format requested by the individual, so long as the information is readily producible in that form or format.⁹ Otherwise, the information must be provided in hard copy or such form agreed upon by the covered entity and the individual, and the covered entity may impose a reasonable fee for providing such information. Second, individuals have the right to request that a covered entity restrict the use and disclosure of their PHI for the purposes of treatment, payment or health care operations.¹⁰ However, as a general matter, covered entities are not required to comply with such a request. Finally, individuals have the right to an accounting of disclosures of their PHI by a covered entity during the previous six years, subject to certain exceptions (e.g., disclosures that have been made to carry out treatment, payment and health care operations are not required to be included in the accounting).¹¹

Notably, ARRA makes modifications to each of these privacy rights for individuals. Under the Act, individuals will have the right to request and receive their information in electronic format from a covered entity if such information is maintained as an electronic health record (EHR), and at a reasonable cost for complying with the request. With respect to requested restrictions on disclosures, covered entities will be required to restrict the disclosure of PHI to a health plan relating to an item or service for purposes of payment or health care operations if the individual has paid for such item or service out-of-pocket in full. In addition, individuals will have the right to receive an accounting of PHI disclosures made by covered entities or their business associates for treatment, payment and health care operations during the previous three years. For current users of EHRs, this requirement will apply for disclosures made on or after January 1, 2014, and for non-users of EHRs, the later of January 1, 2011, or when the covered entity acquires EHRs. The Secretary also may impose a later effective date of not later than 2016 for current users, or not later than 2013 for non-users of EHRs.

Improved Enforcement

The HIPAA Rules authorize the Secretary to impose civil money penalties (CMPs) on any person in violation of the privacy and security standards.¹² The maximum civil fine is \$100 per violation and up to \$25,000 for all similar violations within a given calendar year. CMPs may not be imposed for any of the following reasons: (1) the violation is a criminal offense under HIPAA criminal provisions; (2) the person did not have actual or constructive knowledge of the violation; or (3) the failure to comply was due to reasonable cause and not to willful neglect, and the failure to comply was corrected within a

⁹ See 45 C.F.R. § 164.524.

¹⁰ See 45 C.F.R. § 164.522.

¹¹ See 45 C.F.R. § 164.528.

¹² See 42 U.S.C. § 1320d-5(a).

30-day period.¹³ With respect to certain wrongful disclosures of PHI, the Office of Civil Rights (OCR) may refer the case to the Department of Justice for criminal prosecution.¹⁴ Criminal penalties under the HIPAA Rules include fines up to \$250,000 and up to 10 years in prison.¹⁵

ARRA radically “*ups the ante*” for enforcement of civil violations under HIPAA in a number of consequential ways.

- First, the Act amends HIPAA to permit OCR to pursue an investigation and the imposition of CMPs against any individual for an alleged criminal violation of the HIPAA Rules if the Justice Department has not prosecuted the individual. As such, so long as the individual has not already been prosecuted for the criminal offense, a CMP may be imposed by the OCR. That is, even if the violation constitutes a criminal offense, OCR will be permitted to impose CMPs, provided that the individual has not been prosecuted criminally.
- Second, the Act requires a formal investigation and imposition of CMPs for violations due to willful neglect. The Secretary is required to issue regulations within 18 months of ARRA enactment to carry out this change.
- Third, ARRA authorizes any state attorney general to bring a civil action in federal district court against individuals who violate the HIPAA Rules. The state attorneys general now will have this right of action either to enjoin violations or to seek damages of up to \$100 for each violation and \$25,000 for all similar violations within a calendar year.
- Fourth, the Act establishes four new tiers of CMPs. The CMPs would range from \$100 to \$50,000 for each violation, and \$25,000 to \$1,500,000 for similar violations within a calendar year. The tiers of CMPs would be based on the level of culpability, beginning with no knowledge of the violation to willful neglect. Thus, covered entities and business associates will be subject to considerable penalty amounts for violating the HIPAA Rules.
- Lastly, the Government Accountability Office (GAO) is tasked with recommending to the Secretary a methodology under which harmed individuals under HIPAA would receive a percentage of any CMP or monetary settlement collected with respect to a HIPAA violation. The Secretary, within three years of ARRA enactment, is required to establish by regulation (and based on GAO’s recommendations) the implementation of this methodology.

Together, these enforcement provisions will dramatically change the stakes for compliance with the HIPAA Rules. In addition, the Act sets a stage for greater enforcement of these standards by state attorneys general. As such, covered entities and business associates will be subject to new and more severe sanctions for violations under the law.

¹³ See 42 U.S.C. § 1320d-5(b).

¹⁴ See 42 U.S.C. § 1320d-6(a).

¹⁵ See 42 U.S.C. § 1320d-6(b).

CONCLUSION

Under the changes enacted in ARRA, the scope of coverage, enforcement authority and penalties under the HIPAA Rules are expanded greatly. Whereas business associates have been subject only to compliance with certain required provisions of a business associate agreement, they now are covered directly by the extensive requirements of the HIPAA Rules and ARRA, and subject to enforcement and penalties. The breach notification provisions of the new law will impose costly and burdensome requirements on covered entities in the event of security or privacy breaches regarding PHI. Many entities not previously covered either as covered entities or business associates now will be subject to privacy and security compliance. The new right of action for state attorneys general to sue on behalf of individuals, along with the ability of individuals ultimately to obtain a portion of collected CMPs, will greatly increase the likelihood of enforcement of the HIPAA Rules. Thus, most entities obtaining or maintaining PHI will have significantly heightened responsibilities for providing safeguards for the confidentiality and security of PHI, and they will have more serious penalties for failure to comply with the significantly broader requirements imposed under ARRA.

ARRA Privacy Provisions

Provision	Current Law ¹⁶	ARRA
<p>Definition of Breach</p>	<p>No current provision</p>	<p>Sec. 13400. Defines “breach” as the unauthorized acquisition, access, use or disclosure of protected health information (PHI).</p> <p>Exceptions – A breach does not include</p> <ol style="list-style-type: none"> 1. any unintentional acquisition, access or use by an employee or individual if made in good faith and within the course and scope of the employment <u>and</u> the information is not further acquired, accessed, used or disclosed by any person; or 2. any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility; and 3. any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.
<p>Application of Security Provisions and Penalties to Business Associates</p>	<p>HIPAA civil and criminal penalties apply to covered entities. Covered entities are not liable for, or required to monitor, the actions of their business associates.</p>	<p>Sec. 13401. Applies the HIPAA security standards and the civil and criminal penalties for violating those standards to business associates in the same manner as they apply to covered entities.</p> <p>The Secretary will annually issue guidance, in consultation with industry stakeholders, on the most appropriate security safeguard technologies for protecting information.</p>

¹⁶ Congressional Research Service, *The Health Information Technology for Economic and Clinical Health (HITECH) Act*, Feb. 4, 2009.

Provision	Current Law	ARRA
<p>Notification of Information Breach</p>	<p>HIPAA privacy and security rules do not require covered entities to notify HHS or others of a breach of the privacy, security or integrity of protected health information (PHI). Business associate contracts, however, must include a provision requiring business associates to report to covered entities if they become aware of any security incident or any use or disclosure of PHI that is not provided for by the contract.</p>	<p><i>Sec. 13402.</i> In the case of a breach of unsecured PHI, a covered entity must notify each individual whose information has been, or is reasonably believed to have been, breached. The method and content of the notification is specified by the provision. For a breach of unsecured PHI under the control of a business associate, upon discovery of the breach, the business associate would be required to notify the covered entity.</p> <p>“Unsecured PHI” is PHI that is not secured through the use of a technology or methodology identified by the Secretary as rendering the information unusable, unreadable or indecipherable to unauthorized persons.</p> <p>All breach notifications required by the covered entity and business associate must be made no later than 60 days after discovery (unless it would impede a criminal investigation or national security).</p> <p>The Secretary must also be notified by the covered entity of such breaches. If more than 500 individuals are involved, the Secretary must be notified immediately and notice must be made to the local media. With respect to less than 500 individuals, the covered entity may report breaches on an annual basis.</p> <p>The Secretary must post publicly a list of the covered entities involved in breaches of more than 500 individuals.</p> <p>The Secretary must promulgate interim final regulation relating to the breach requirements no later than 180 days following enactment to be effective 30 days following.</p> <p>No later than one year following the enactment and annually thereafter, the Secretary must report to Congress on the nature and number of breaches for which the Secretary is notified and the actions taken.</p>
<p>Privacy Education</p>	<p>The privacy rule requires each covered entity to designate a privacy official for the development and implementation of its policies and procedures.</p>	<p><i>Sec. 13403.</i> The Secretary will designate a “privacy advisor” in each regional office of HHS to offer education and guidance to covered entities and business associates.</p> <p>The Office of Civil Rights (OCR) shall develop and maintain a national education initiative to educate the public about their privacy rights.</p>
<p>Application of Privacy Provisions and Penalties to Business Associates</p>	<p>HIPAA civil and criminal penalties apply to covered entities. Covered entities are not liable for, or required to monitor, the actions of their business associates.</p>	<p><i>Sec. 13404.</i> Business associates would only be permitted to use or disclose PHI if such action was in compliance with their written contract.</p> <p>Applies the HIPAA privacy provisions and the civil and criminal penalties for violating those standards to business associates in the same manner as they apply to covered entities.</p>

Provision	Current Law	ARRA
<p>Patient's Privacy Rights</p>	<p>The privacy rule establishes a number of federal privacy rights, including (1) the right of access to one's own PHI; (2) the right to amend or supplement one's PHI; (3) the right to request that a covered entity restrict the use and disclosure of one's PHI for the purposes of treatment, payment, or other health care operations; and (4) the right to an accounting of PHI disclosures (other than for treatment, payment or health care operations, or pursuant to an authorization). The privacy rule incorporates a minimum necessary standard. However, there are a number of circumstances in which the minimum necessary standard does not apply, such as with respect to disclosures or requests by a health care provider for treatment purposes.</p> <p>Disclosures of a "limited data set" for certain specified purposes (e.g., research) are permitted pursuant to a data use agreements with the recipient. A limited data set has most direct identifiers removed and is considered to pose a low privacy risk.</p>	<p>Sec. 13405.</p> <p>Requested Restrictions on Certain Disclosures: Permits individuals to request that their PHI regarding a specific item or service not be disclosed by a covered entity to a health plan for purposes of payment or health care operations, unless otherwise required by law, if the individual has paid in full out-of-pocket for the item or service. Under these circumstances, the covered entity must comply with the request.</p> <p>Limiting Disclosures to the Limited Data Set or the Minimum Necessary: With respect to the use, disclosure or request of PHI, covered entities must make reasonable efforts to limit such PHI to the "limited data set" (as defined by HIPAA) or the "minimum necessary" to accomplish the intended purpose of such use, disclosure or request.</p> <p>The Secretary shall issue guidance on what constitutes "minimum necessary" no later than 18 months after enactment. In issuing guidance relating to what constitutes "minimum necessary," the Secretary shall take into consideration the information necessary to improve patient outcomes and to detect, prevent and manage chronic disease.</p> <p>Permits the covered entity or business associate to determine what constitutes the minimum necessary to accomplish the intended purpose of disclosures.</p> <p>Accounting of Certain PHI: In the event that a covered entity uses or maintains an electronic health record (EHR) with respect to PHI, individuals will have the right to receive an accounting of PHI disclosures made by covered entities for treatment, payment and health care operations during the previous three years.</p> <p>The Secretary must promulgate regulations on what information must be included in the accounting within six months of adopting HIT technical standards on accounting for disclosures. The regulations must take into account the interest of individuals and the administrative burden.</p> <p>In response to a request, a covered entity must provide either</p> <ol style="list-style-type: none"> 1. an accounting for disclosures that are made by the covered entity and by a business associate acting on behalf of the covered entity; or 2. an accounting for disclosures that are made by the covered entity and a list of all business associates acting on behalf of the covered entity. (A business associate included on the list must provide the accounting as required for covered entities if an individual requests such accounting from the business associate). <p>Covered entities that currently use EHR must comply with this requirement with respect to disclosures of PHI made by a covered entity on and after January 1, 2014. For covered entities that acquire EHR after January 1, 2009, the requirement will apply on January 1, 2011 or the date that the covered entity acquires EHR.</p>

Provision	Current Law	ARRA
<p>Patient's Privacy Rights (cont'd)</p>		<p>The Secretary may set a later effective date for current users of EHR and users of EHR after January 1, 2009, if the Secretary determines it to be necessary. However, in no case, can the date be later than 2016 for current users, or 2013 for other users.</p> <p>Prohibition on Sale of EHR or PHI: Clarifies that certain uses and disclosures of PHI are not permitted without a valid authorization, such as the sale of PHI, unless for</p> <p>(1) public health activities; (2) research and the price charged reflects the costs of preparation and transmittal data; (3) treatment of the individual subject to any regulations the Secretary may promulgate to prevent health information from inappropriate access, use or disclosure; (4) health care operations; (5) activities performed by a business associate pursuant to a business associate agreement; (6) the provision of a copy of an individual's PHI to the individual; and (7) other activities determined appropriate by the Secretary.</p> <p>The Secretary must promulgate regulations to for this section within 18 months of enactment, to be effective six months after promulgation. In promulgating the regulations to carry out this prohibition, with respect to the public health activities exception, the Secretary must evaluate the impact of restricting the exception to require that the price charged reflects the costs of the preparation and transmittal of data relating to the public health activity, including those conducted by the FDA. In addition, the Secretary may apply this restriction if the Secretary determines that such restriction would not impede public health activities.</p> <p>Access to Certain Information in Electronic Format: Individuals may receive electronic copies of their PHI used or maintained by a covered entity in electronic format if the entity uses an EHR, at a cost not to exceed the entity's labor costs. An individual may also choose to direct the covered entity to transmit copies of their information to an entity or person designated by the individual, so long as the choice is clear, conspicuous and specific.</p>

Provision	Current Law	ARRA
<p>Health Care Operations –Marketing and Fundraising</p>	<p>“Health care operations” is broadly defined and includes activities such as case management, quality assessment, underwriting, legal services, business planning, customer services and fundraising.</p> <p>As a general matter, a covered entity may not use or disclose health information for its own marketing activities without authorization. A communication about a product or service to a recipient to encourage the recipient to purchase or use the product or service is within the definition of marketing. However, marketing communications made by a covered entity (or its business associate), for example, to describe a health-care related product or service, for treatment of an individual, or for case management or care coordination, are excluded from this definition and, therefore, do not require a patient’s authorization, even if the covered entity is paid by a third party to engage in such activities.</p>	<p>Sec. 13406.</p> <p>Marketing: Clarifies the definition of marketing under HIPAA. A marketing communication by a covered entity or business associate that is about a product or service that encourages recipients of the communication to purchase or use the product or service is not considered a health care operation, unless the communication relates to, for example, a health-care related product or service, treatment for an individual or case management or care coordination.</p> <p>Prohibits a covered entity or business associate from receiving any payment for marketing communications relating to a health care-related product or service, treatment for an individual or case management or care coordination unless</p> <ol style="list-style-type: none"> 1. the communication describes only a drug or biologic that is currently prescribed for the recipient of the communication and any payment received by the covered entity is reasonable in amount; 2. the communication is made by a covered entity and the covered entity obtains a valid authorization from the recipient of the communication; or 3. the communication is made on behalf of the covered entity, and the communication is consistent with the written contract between the business associate and covered entity. <p>A “reasonable cost” will be defined by the Secretary in regulation.</p> <p>Fundraising: The Secretary shall provide that individuals may opt-out of any fundraising communication authorized under the definition of “health care operations.”</p>
<p>Personal Health Record (PHR) Breach Notification Requirement – PHR Vendors and Non-HIPAA Covered Entities</p>	<p>The HIPAA privacy and security rules apply to covered entities and, through written contracts, to their business associates.</p>	<p>Sec. 13407. In the case that an individual’s unsecured PHR identifiable information is breached, PHR vendors must notify the affected individual and the Federal Trade Commission (FTC). Third party service providers that provide services to PHR vendors are required to notify the vendor of any such breach.</p> <p>“Unsecured PHR identifiable health information” is PHR health information that is not protected through the use of a technology or methodology specified in guidance issued by the Secretary.</p> <p>The FTC must also notify the Secretary of such breach.</p> <p>Provides the FTC with the enforcement authority regarding breaches of health information maintained by PHR vendors.</p> <p>The FTC must promulgate interim final regulations by not later than 180 days after enactment.</p> <p>Any subsequent legislation put forth by Congress establishing new requirements for notification in the case of a breach by non-covered entities or non-business associates will supersede this section.</p>

Provision	Current Law	ARRA
<p>Business Associate Contracts</p>	<p>No current provision</p>	<p><i>Sec. 13408.</i> Requires organizations that contract with covered entities for the purpose of exchanging electronic PHI, such as Health Information Exchanges, Regional Health Information Organizations, E-Prescribing Gateways and vendors of PHRs who have entered contracts with covered entities to have business associate agreements with those entities.</p>
<p>Criminal Penalties for Wrongful Disclosures</p>	<p>Under HIPAA, only covered entities can be found criminally liable for wrongful disclosures of individually identifiable information.</p>	<p><i>Sec. 13409.</i> Amends HIPAA to clarify that criminal penalties for wrongful disclosure of individually identifiable health information apply to individuals who without authorization obtain or disclose such information maintained by a covered entity, whether they are employees or not.</p>
<p>Improved Enforcement</p>	<p>The Secretary is authorized to impose civil monetary penalties on any person failing to comply with the privacy and security standards.</p> <p>Civil money penalties may not be imposed if (1) the violation is a criminal offense under HIPAA's criminal penalty provisions; (2) the person did not have actual or constructive knowledge of the violation; or (3) the failure to comply was due to reasonable cause and not to willful neglect, and was corrected within 30 days.</p> <p>HIPAA's criminal penalties include fines of up to \$250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.</p>	<p><i>Sec. 13410.</i> Amends HIPAA to permit OCR to pursue an investigation and the imposition of civil monetary penalties against any individual for an alleged criminal violation of the HIPAA standards if the Department of Justice has not already prosecuted the individual.</p> <p>Requires a formal investigation of complaints and the imposition of civil monetary penalties for violations due to willful neglect.</p> <p>The Secretary, within three years of enactment, would be required to establish by regulation (based on Government Accountability Office (GAO) recommendations) a methodology to distribute a percentage of any collected penalties to harmed individuals.</p> <p>Replaces HIPAA's existing civil monetary penalties with four tiers of penalties based on the level of knowledge of the violation, the highest of which would impose a fine of up to \$50,000 per violation, and up to \$1,500,000 for all such violations of an identical requirement or prohibition during a calendar year.</p> <p>Preserves the current requirement that a civil fine would not be imposed if the violation was due to reasonable cause and corrected within 30 days.</p> <p>Authorizes state attorneys general to bring a civil action in federal district court against individuals who violate the HIPAA privacy and security standards.</p> <p>Permits the OCR to continue to use corrective action without a penalty in cases where the person did not know, and by exercising reasonable diligence would not have known, about the violation.</p>
<p>Compliance Audits</p>	<p>The Secretary is authorized to conduct compliance reviews to determine whether covered entities are complying with HIPAA standards.</p>	<p><i>Sec. 13411.</i> Requires the Secretary to perform periodic audits to ensure compliance with the HIPAA privacy and security standards and the requirements set forth in this legislation.</p>

Provision	Current Law	ARRA
<p>Preemption of State Law</p>	<p>The HIPAA security standards preempt any contrary provision of state law, with certain specified exceptions (e.g., public health reporting). However, the privacy rule does not preempt a contrary provision of state law that is more protective of patient medical privacy.</p>	<p><i>Sec. 13421.</i> Applies the HIPAA preemption provisions to the privacy subtitle of this bill and preserves the HIPAA privacy and security standards to the extent they are consistent with this subtitle.</p> <p>Requires the Secretary, by rulemaking, to amend the HIPAA standards as necessary to make them consistent with the legislation's privacy and security provisions.</p> <p>Nothing in the privacy provisions will constitute a waiver of any privilege otherwise applicable to an individual with respect to the PHI of such individual.</p>
<p>Effective Date</p>		<p><i>Sec. 13423.</i> Except as otherwise specified, the privacy and security provisions would become effective 12 months after enactment.</p>
<p>Studies, Reports, and Guidance</p>	<p>Any person who believes a covered entity is not complying with the privacy rule may file a complaint with HHS. HIPAA does not require the Secretary to issue a compliance report.</p>	<p><i>Sec. 13424.</i> Requires that the Secretary submit an annual report to Congress on the number and nature of complaints of alleged violations and how they were resolved, including the imposition and amount of civil money penalties; the number of audits performed; and other elements.</p> <p>Requires the Secretary and FTC to conduct a study and submit a report to Congress on the application of privacy and security requirements to non-HIPAA covered entities.</p> <p>Requires the Secretary to issue guidance on how best to implement the requirements for the de-identification of PHI.</p> <p>Requires the GAO to study and report on the disclosures of PHI made for treatment purposes and best practices used by entities and States for such disclosures.</p> <p>Requires GAO to submit a report to Congress and the Secretary on the impact of these privacy provisions on health insurance premiums, overall health care costs, adoption of EHRs by providers, reduction in medical errors and other quality improvements.</p> <p>Requires the Secretary to study the definition of "psychotherapy notes" with regard to including test data that is related to direct responses, scores, items, forms, protocols, manuals or other materials that are part of a mental health evaluation, as determined by a mental health professional providing treatment or evaluation. The Secretary may, based on the study, issue regulations to revise such definition.</p>

If you would like to receive future *Health Care Advisories* electronically, please forward your contact information including e-mail address to healthcare.advisory@alston.com. Be sure to put “**subscribe**” in the subject line.

For further guidance on HIPAA security or privacy compliance relating to the changes implemented by ARRA, please contact one of the attorneys or advisors listed below:

Washington Office

Jacqueline C. Baratian
202.756.3484
jacqueline.baratian@alston.com

Jennifer L. Butler
202.756.3326
jennifer.butler@alston.com

Elinor A. Hiller
202.756.3401
elinor.hiller@alston.com

Laura E. Holland
202.239.3980
laura.holland@alston.com

Peter M. Kazon
202.756.3334
peter.kazon@alston.com

Stephanie A. Kennan
Senior Public Policy Advisor
202.756.3159
stephanie.kennan@alston.com

Keavney F. Klein
202.239.3981
keavney.klein@alston.com

Rudy S. Missmar
202.756.3034
rudy.missmar@alston.com

Mark Rayder
Senior Public Policy Advisor
202.756.3562
mark.rayder@alston.com

Colin T. Roskey
202.756.3436
colin.roskey@alston.com

Marc J. Scheineson
202.756.3465
marc.scheineson@alston.com

Thomas A. Scully
202.756.3459
thomas.scully@alston.com

Donald E. Segal
202.756.3449
donald.segal@alston.com

Tamara R. Tenney
202.756.3489
tamara.tenney@alston.com

Julie K. Tibbets
202.756.3444
julie.tibbets@alston.com

Timothy P. Trysla
202.756.3420
tim.trysla@alston.com

Tiffani V. Williams
202.756.3412
tiffani.williams@alston.com

Marilyn Yager
Senior Public Policy Advisor
202.756.3341
marilyn.yager@alston.com

Atlanta Office

Donna P. Bergeson
404.881.7278
donna.bergeson@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Jeffrey K. Hester
404.881.4254
jeff.hester@alston.com

Robert C. Lower
404.881.7455
bob.lower@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

D'Andrea J. Morning
404.881.7538
dandrea.morning@alston.com

Robert D. Stone
404.881.7270
robert.stone@alston.com

Michelle A. Williams
404.881.7594
michelle.williams@alston.com

ATLANTA

One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404.881.7000

CHARLOTTE

Bank of America Plaza
Suite 4000
101 South Tryon Street
Charlotte, NC 28280-4000
704.444.1000

DALLAS

Chase Tower
Suite 3601
2200 Ross Avenue
Dallas, TX 75201
214.922.3400

LOS ANGELES

333 South Hope Street
16th Floor
Los Angeles, CA 90071-3004
213.576.1000

NEW YORK

90 Park Avenue
New York, NY 10016-1387
212.210.9400

RESEARCH TRIANGLE

Suite 600
3201 Beechleaf Court
Raleigh, NC 27604-1062
919.862.2200

SILICON VALLEY

Two Palo Alto Square
Suite 400
3000 El Camino Real
Palo Alto, CA 94306-2112
650.838.2000

VENTURA COUNTY

Suite 215
2801 Townsgate Road
Westlake Village, CA 91361
805.497.9474

WASHINGTON, D.C.

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202.756.3300

www.alston.com

© Alston & Bird LLP 2009