



**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
Section 13400 – Definitions	<p>Adds new definitions for:</p> <ul style="list-style-type: none"> • Breach* • Electronic health record (“EHR”) • National Coordinator • Personal health record (“PHR”) • State • Vendor of personal health record <p>Reiterates definitions for other terms by cross-referencing to current regulations</p> <p>*Breach: “unauthorized acquisition, access, use, or disclosure of [PHI] which compromises the security or privacy of such information, <u>except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.</u>”</p> <p>Exceptions include: (i) unintentional acquisition, access or use by an employee of a covered entity (“CE”) or business associate (“BA”) made in the scope of employment (or other relationship) and in good faith, provided information is not further used, disclosed, etc; (ii) inadvertent disclosure by an authorized person to an unauthorized person at same facility, provided not further used, disclosed, etc.</p>	<p>For the most part, these are new definitions, so not included in current regulations.</p>	<p>Definitions for EHR, National Coordinator, PHR, State and vendor of PHR are included to address the new provisions about EHRs and the ability of State AGs to prosecute for HIPAA violations.</p> <p>Definition for breach added to address new notification provision, so impact on when there is obligation to notify. Note that, if information cannot be retained, it is not a breach. Also, note exceptions for inadvertent disclosures within a facility and unintentional acquisitions within course of employment.</p>	<p>N/A</p>
Section 13401 – Application of Security Provisions and Penalties to BAs; Annual Guidance on Security Provisions	<p>(a & b) Current HIPAA Security Rule provisions regarding administrative, physical and technical safeguards, as well as those regarding policies/procedures and documentation are applicable to BAs. Civil and criminal penalties for violating those standards are applied to BAs in same way as to CEs. New requirements that relate to security and are applicable to CE shall</p>	<p>Currently, Security Standards and penalties only apply to CEs, although BAs are subject to them contractually through the BAA.</p>	<p>Significant impact on business associates, as they are now subject directly to many provisions of HIPAA Security Rule and to civil and criminal penalties in same way as covered entities. BAs will need to</p>	<p>Falls within general requirement that Secretary enact regulations to implement changes to Privacy and Security Rules, but no required timeline. Expect</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
	<p>apply to BA and “be incorporated into business associate agreement.”</p> <p>(c) Secretary shall annually issue guidance on most effective and appropriate technical safeguards (including the use of standards being considered by HIT Policy Committee under ARRA to render PHI unidentifiable).</p>	<p>No annual guidance exists currently.</p>	<p>conduct risk assessments and draft HIPAA Security policies.</p> <p>Possible impact on BAAs – may need to restructure existing BAAs to include security rule provisions (including civil and criminal penalties); contracts going forward will need to be revised. Entities will want to wait for regulations to determine how to modify agreements.</p> <p>New guidance should help clarify required safeguards (a benefit), but may require adoption of new technologies in order to meet the standards.</p>	<p>regulations will address new elements that should be included in the BA. Also expect to see regulations applying Security Standards to BAAs and directing Secretary to issue annual guidance.</p>
<p>Section 13402 – Notification in Case of Breach</p>	<p>(a) In general, CEs that access, maintain, retain, modify, record, store, destroy or otherwise use, or disclose unsecured PHI must notify individuals whose <u>unsecured PHI</u> has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a breach discovered by the CE.</p> <p>(b) Same provision as (a) with respect to BAAs, but they must notify CEs in event of breach, including identification of each individual whose unsecured PHI is impacted.</p>	<p>Only current regulation is provision requiring mitigation (no current requirement for notification).</p>	<p>Very significant impact – once guidance is issued as to what technologies and methodologies are acceptable, CEs and BAAs will need to determine whether to use them (which could be costly) so as not to hold any unsecured PHI. If entity cannot so protect PHI, will be subject to breach notification</p>	<p>No later than August 16, 2009, Secretary must promulgate interim final regulations. Regulations will address definition of unsecured PHI, notification requirements, content of notification, timeliness, etc.</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
	<p>(c) A breach is treated as discovered by a CE or BA as of the first day on which it is known or should reasonably have been known to have occurred (including any person, other than individual committing breach, who is employee, officer or agent).</p> <p>(d) Notifications must be made “without unreasonable delay” but no later than 60 calendar days after discovery (burden of proof on CE or BA).</p> <p>(e) Four types of notice required:</p> <ul style="list-style-type: none"> • <u>Individual</u> must be notified by 1st class mail or, if not possible, by substitute form (including, if there are 10 or more persons who cannot be contacted via mail, posting on home page of entity’s website or notice in major print or broadcast media); • <u>Media</u> notice required if more than 500 residents of a state or jurisdiction are impacted; • <u>Secretary</u> must be notified; if more than 500 individuals impacted, notice must be provided immediately, but if less than 500 individuals, CE can maintain a log and submit annually; • <u>HHS website</u> – will publish each CE involved in a breach if more than 500 individuals impacted. <p>(f) Content – notice shall include description of what happened, types of unsecured PHI involved,</p>		<p>requirements (including media notice and publication on HHS website if breach impacts over 500 individuals).</p> <p>This section follows movement by many states to require individual notification when personal information is breached.</p>	<p>Provisions will apply to breaches discovered on or after 30 days after the date of publication of the interim regulations (no later than September 15, 2009).</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
	<p>steps an individual should take to protect himself/herself, what CE is doing to mitigate, contact person.</p> <p>(g) Delay of notice for law enforcement purposes (if notice would impede criminal investigation).</p> <p>(h) Defines “unsecured PHI” – PHI that is not secured through use of a technology or methodology specified by Secretary to render PHI unusable, unreadable or indecipherable (which is expected to occur no later than 60 days after enactment); NOTE: if no guidance issued, must use standards developed or endorsed by standards developing organization accredited by American National Standards Institute</p> <p>(i) Secretary shall annually report to Congress regarding number and nature of breaches and actions taken in response</p> <p>(j) Secretary must promulgate interim final regulations by 180 days after enactment and section applies to breaches discovered 30 days after publication of such regulations</p>			
<p>Section 13403 – Education on Health Information Privacy</p>	<p>(a) Within 6 months, Secretary must appoint one individual in each regional office to serve as Privacy Advisor, offering guidance and education to CEs, BAs and individuals on rights and responsibilities related to HIPAA privacy and security.</p> <p>(b) No later than 12 months post-enactment, OCR must develop and maintain a national education initiative.</p>	<p>Not addressed in current regulations</p>	<p>No expected impact</p>	<p>N/A</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
Section 13404 – Application of Privacy Provisions and Penalties to BAs	<p>Extends certain requirements related to HIPAA privacy, and the civil and criminal penalties for violating those standards or for using/disclosing protected health information in a manner contrary to the business associate agreement, to BAs; new requirements relating to privacy now applicable to BAs “shall be incorporated into the business associate agreements.”</p> <p>Provisions of 45 C.F.R. 164.504(e)(ii) (requiring CE to take certain steps upon becoming aware of violation of BAA by BA) now apply to BA upon becoming aware of violation by CE.</p>	<p>Under the current regulations, CEs may disclose PHI to BAs only pursuant to a written contract, pursuant to which the BA promises to safeguard the information. Violations cannot be enforced directly against BAs, but CEs are required to terminate the contract or notify HHS if they learn of a breach by BA that cannot be remedied.</p>	<p>Significant impact on BAs, as they are now subject to many provisions of the HIPAA Privacy Rule and to penalties for violating such provisions.</p> <p>BAA templates likely will need to be changed and new BAA templates created to account for new provisions, including making the termination provision mutual in the event of a breach of the contract (currently, BAAs give only CE ability to terminate or notify HHS in event of breach).</p>	<p>Falls within general requirement that Secretary enact regulations to implement changes to Privacy and Security Rules, but no required timeline.</p>
Section 13405 – Restrictions on Certain Disclosures and Sales of Health Information; Accounting of Certain PHI Disclosures; Access to Certain Information in Electronic Format	<p>(a) If an individual requests a restriction in the disclosure of PHI for treatment, payment or health care operations (“HCOs”), CE <u>must comply</u> if disclosure is to health plan for purpose of payment or HCO and the PHI relates to an item or service for which the provider was paid in full by the individual (unless required by law).</p>	<p>(a) Currently, § 164.522 does not require a CE to agree to any request for restriction, but if it does, it must follow the restriction (unless emergency treatment is needed)</p>	<p>(a) Not likely to be significant impact, as individuals do not often request such restrictions; however, it does take away autonomy of covered entities.</p>	<p>(a) Falls within general requirement that Secretary enact regulations to implement changes to Privacy and Security Rules, but no required timeline.</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
	<p>(b) Within 18 months of enactment, the Secretary shall issue guidance on what constitutes “minimum necessary.” Until that point, a CE shall be in compliance with minimum necessary requirements only if it limits PHI to an LDS or, if needed, to the minimum necessary to accomplish the reason for the use or disclosure, as determined by the CE. The exceptions to minimum necessary are retained. Does not apply to de-identified PHI.</p> <p>(c) Accounting provision for Electronic Health Records (“EHR”) - CE must provide an accounting of disclosures made for treatment, payment or HCOs for three year period if disclosure made by EHR. New regulations required w/in 6 months re: what information must be collected. As with other accountings, CE can choose to provide list of all BAs and have individual contact BA directly, in which case BA must make accounting. If CE has an electronic health record as of 1/1/2009, this section will apply as of 1/1/2014; otherwise it will apply to disclosures on or after the later of 1/1/2011 or the date the EHR is acquired (unless Secretary specifies later date in the regulations, which can’t be later than 2016 or 2013, respectively).</p>	<p>(b) Currently, § 164.502(b)(1) requires that a CE make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of a use, disclosure or request.</p> <p>(c) Currently, § 164.528 provides an exception to the accounting provision for disclosures to carry out treatment, payment and health care operations.</p>	<p>(b) Possible significant impact once regulations are released, as may create more administrative work for CEs as they use, disclose and request information.</p> <p>(c) Significant impact on EHR systems. New systems will need to include technology to account for such disclosures, while old systems will need to be updated (if necessary) so that they can do so. Once the technology exists, it should not be too difficult for CEs to provide the accounting, as they will be able to run it automatically from the system. CEs will need to run separate accountings for different types of disclosures b/c most accountings must cover a six year period. Particularly relevant for clients who are EHR companies, or clients who</p>	<p>(b) Secretary must issue guidance within 18 months of enactment (August 17, 2010), which will specify what constitutes “minimum necessary.” Provision under ARRA sunsets upon issuance of guidance.</p> <p>(c) No later than six months after the date on which HHS adopts technical standards on accountings, Secretary must promulgate regulations on what information shall be collected – no later than June 30, 2010. Regulations may also extend implementation date.</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
	<p>(d) Neither CE nor BA may receive remuneration for sale of PHI without authorization specifically so allowing. Exceptions include sales for following purposes:</p> <ul style="list-style-type: none"> • Public health activities • Research and price reflects cost of preparation and transmittal of data • Treatment (unless prohibited by regulation); • Health care operations (only for sale, transfer, merger or consolidation) • Remuneration provided to BA for activities involving exchange of PHI done by BA under BAA; • To provide individual with copy of PHI; • Any other exceptions permitted by regulations promulgated by Secretary. <p>(e) With respect to access provisions for EHR, individual shall have right to obtain copy in electronic format and, if desired, to direct CE to transmit copy to an entity or person designated (provided designation is clear, conspicuous and specific) and any fee imposed shall not be greater than labor costs of responding to request.</p>	<p>(d) Current regulations do not prohibit the receipt of remuneration in exchange for PHI, provided the disclosure of PHI is permitted under HIPAA. However, in order for an entity to sell PHI for marketing purposes, there must be an authorization and the authorization must include a statement about remuneration.</p> <p>(e) Current access provisions do not specifically address EHRs.</p>	<p>have or who are thinking about getting an EHR.</p> <p>(d) New regulations may not have a significant impact because most of the current arrangements where a CE is receiving remuneration in exchange for the disclosure of PHI would fit under one of the exceptions (such that authorization would not be required). One situation that may <u>not</u> be covered by an exception is a disclosure of PHI to another entity for that other entity’s health care operations.</p> <p>(e) CEs with EHRs will need to be able to provide access to PHI electronically. Need to make sure provision of access is consistent with Security Rule (i.e. technology to protect EPHI as it is transferred). Authorization likely not required in order to transmit to someone who is not the</p>	<p>(d) No later than August 17, 2010, Secretary shall promulgate regulations carrying out this section, which regulations shall become effective six months later (no later than February 17, 2011). New regulations may contain additional exceptions where sale of PHI is allowed without authorization.</p> <p>(e) Access provisions of Privacy Rule likely will be amended to include this.</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
			individual, provided that the identity of the person is clearly designated.	
Section 13406 – Conditions on Certain Contacts as Part of Health Care Operations	<p>(a) Clarifies that a marketing communication by a CE or BA about a product or service that encourages the recipient to purchase or use the product or service may not be considered a health care operation, unless the communication relates to a health care-related product or service, treatment or case management (i.e. falls under subparagraphs (i) – (iii) of paragraph (1) of definition of marketing). Even communications about health-related products, treatment or case management may not be health care operations if remuneration involved unless: (i) communication is about drugs or biologics currently being prescribed where payment for making communication is reasonable in amount; (ii) communication is made by CE pursuant to authorization; or (iii) communication is made by BA pursuant to BAA.</p> <p>(b) Regulations shall provide that fundraising communications must include an opt-out and that election to opt-out shall be treated as a revocation of authorization.</p>	<p>(a) Currently, communications about health-related products or services in paragraph (i) – (iii) of paragraph 1 of the definition of marketing are excepted from the definition of marketing. No language about whether these communications are health care operations. Current definition of marketing includes communications by CEs in exchange for remuneration to another entity for the other entity to market its own products or services.</p> <p>(b) § 164.514(f) permits a CE to disclose to a BA or institutionally related foundation, certain information without an authorization. Any fundraising materials must include a description of how an individual can opt-out.</p>	<p>(a) Potentially significant impact on arrangements that currently fall under health-related product or services exceptions to definition of marketing. While such communications may be treated as health care operations, they may not be treated so if remuneration is involved (unless fall within one of the exceptions), which means authorization will be required.</p> <p>(b) Impact of change is that CEs must treat decision to opt-out as a revocation of an authorization, meaning that all of the protections under § 164.508 for revocations of authorization will apply (including that individual may not be denied treatment).</p>	<p>(a) Regulations must set forth what “reasonable amount” is for payment relating to a communication about a drug or biologic currently being prescribed to the individual. Definition of marketing and/or of health care operations may change to reflect clarification. No known timeline.</p> <p>(b) Regulations will specify that individuals who opt-out of fundraising will be protected in the same way as individuals who revoke authorizations. No set timeline.</p>
Section 13407 – Temporary	(a) Vendors of personal health records, entities that market on websites of such vendors, entities	Currently, the HIPAA Privacy Rule does not	Significant impact for vendors of personal health	Federal Trade Commission must

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
<p>Breach Notification Requirement for Vendors of Personal Health Records and other non-HIPAA Covered Entities.</p>	<p>that market on CE websites that offer personal health records and entities that are not CEs and that access or send information to personal health records must notify individuals and the FTC in the event of a breach of unsecured PHR identifiable health information.</p> <p>(b) Most third party service providers that provide services to any entity listed in (a) must notify the entity in the event of a breach of unsecured PHR identifiable health information, including the identify of any individual affected.</p> <p>(c) The requirements for breach notification specified in Section 13402 shall apply to breaches in this section, as specified by the FTC.</p> <p>(d) Upon notification of a breach, FTC must notify Secretary.</p> <p>(e) Violation of this section shall be treated as an unfair and deceptive act or practice in violation of FTC Act.</p> <p>(f) Sets forth definitions of breach of security (acquisition of information without authorization), PHR identifiable health information (individually identifiable health information provided by or on behalf of the individual that identifies or is likely to identify the individual), unsecured PHR identifiable health information (same as unsecured PHI but for PHR identifiable health information).</p> <p>(g) FTC must promulgate interim final regulations</p>	<p>contain any breach notification requirements, nor does it apply directly to non-covered entities.</p>	<p>records (including EHRs), as well as the other entities included in this provision – significant administrative burden, potential penalties and public relations issues.</p>	<p>promulgate interim final regulations no later than August 16, 2009 (6 months following enactment), which will apply to breaches of security discovered on or after 30 days later (no later than September 15, 2009).</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
	by 180 days after enactment, which will apply to breaches discovered 30 days later. Sunset provision if Congress enacts new legislation establishing requirements for notification in the event of a breach of security applying to entities that are not CEs or Bas.			
Section 13408 – Business Associate Contracts required for Certain Entities	Any organization providing data transmission of PHI and that requires access on a routine basis to such PHI (such as Regional Health Information Organizations, Health Information Exchange Organizations, and EHR vendors) shall be treated as a BA and must enter into a BAA.	Current law does not specifically include or exclude these organizations in the definition of a BA.	Not too significant of an impact, as most covered entities likely treat such organizations already as a BA. Big impact for any such organizations not treated as BA currently, as they will now be subject to HIPAA directly through the new legislation.	Falls within general requirement that Secretary enact regulations to implement changes to Privacy and Security Rules, but no required timeline.
Section 13409 – Clarification of Application of Wrongful Disclosures Criminal Penalties	Amends HIPAA criminal penalties provision to make clear it applies to a person (including an employee or other individual) and not just a CE (or someone who would be liable under an agency theory).	The HIPAA 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.	New provision basically clarifies that all individuals are subject to HIPAA criminal provisions, not just covered entities and employees.	Falls within general requirement that Secretary enact regulations to implement changes to Privacy and Security Rules, but no required timeline.
Section 13410 – Improved Enforcement	(a) Requires Secretary to formally investigate complaints and impose penalties for any violation due to willful neglect. Fact that the act is subject to criminal enforcement does not bar civil enforcement (unless penalty has been imposed). (b) Secretary must promulgate regulations under subsection (a) within 18 months of enactment (no	HIPAA authorizes Secretary to impose civil monetary penalties on any person who violates the regulations in amount of \$100 per violation, up to \$25,000 for all violations of an identical requirement or	This section is clearly in response to OCR’s perceived lack of enforcement in this area. Potentially significant to any person who violates the act, given State enforcement, higher	No later than August 17, 2010, Secretary must promulgate regulations regarding noncompliance due to willful neglect. GAO must submit a report to HHS by August 17,

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
	<p>later than August 17, 2010). Subsection (a) applies to penalties imposed on or after February 17, 2011.</p> <p>(c) Any civil monetary penalties or settlements shall be transferred to the Office of Civil Rights (“OCR”) to be used for purposes of enforcing HIPAA. Within 18 months (no later than August 17, 2010), GAO shall submit a report including recommendations under which a victim may receive some of this money. Based on report, Secretary (no later than February 17, 2012) must establish by regulation a methodology to distribute a percentage of any collected penalties to harmed individuals.</p> <p>(d) Institutes tiered increase in amount of penalties, depending on nature and extent of violation and harm (different tiers depending on whether person did not know of noncompliance, violation was due to reasonable cause or violation was due to willful neglect). Highest tier imposes violations of \$50,000 for each violation, up to a maximum of \$1.5 million in a calendar year. New amounts apply to violations occurring after the date of enactment (February 17, 2009).</p> <p>(e) Permits State Attorneys General to bring civil action on behalf of State residents whose interests have been threatened or adversely affected by a violation of HIPAA, unless Secretary has already instituted such action. Damages are \$100 per violation up to \$25,000 per year, and court may award attorney’s fees. State is required to notify</p>	<p>prohibition during a calendar year. Civil monetary penalties may not be imposed if (1) the violation is a criminal offense under HIPAA; (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 w/in 30 days the failure to comply was discovered (or should have been discovered).</p> <p>OCR may also refer certain cases to DOJ for criminal prosecution, including fines up to \$250,000 and 10 years in prison.</p>	<p>penalties of federal enforcement, etc.</p>	<p>2010, including recommendations for a methodology for providing some measure of compensation to victims. Secretary must promulgate regulations by February 17, 2012 regarding victim compensation.</p> <p>Note that, while majority of these provisions are not effective until February 17, 2010, the new tiered system of penalties, as well as the State AG right of enforcement, will apply to violations occurring after February 17, 2009.</p>

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
	<p>Secretary and provide copy of complaint (unless not feasible) and Secretary may intervene. This subsection is effective for violations occurring after the date of enactment (February 17, 2009).</p> <p>(f) Clarifies that OCR may continue to use corrective action without penalty in cases where the person did not know (and would not have known with reasonable diligence) of the violation.</p>			
Section 13411 – Audits	Secretary shall conduct periodic audits of covered entities and business associates to ensure compliance.	Current regulations permit, but don’t require, the Secretary to conduct audits.	This could be significant to CEs and BAs. The OIG conducted some HIPAA Security audits this past year. This indicates that such audits likely may become more regular.	Falls within general requirement that Secretary enact regulations to implement changes to Privacy and Security Rules, but no required timeline.
Section 13421 – Relationship to Other Laws	Applies preemption provision of 42 U.S.C. 1320d-7 to new provisions. Standards governing privacy and security of PHI shall remain in effect to the extent they are consistent with new provisions and Secretary shall amend existing regulations to incorporate new provisions.	Under 42 U.S.C. 1320d-7, the security standards preempt any contrary provision of state law, with certain specified exceptions (e.g., public health reporting). Pursuant to HIPAA, the privacy rule does not preempt a contrary provision of state law that is more protective of patient privacy.	<p>Essentially clarifies that the new provisions will be subject to HIPAA preemption provisions. Also requires Secretary to amend regulations to address new provisions.</p> <p>Most likely impact will be with respect to whether new breach provisions preempt new state law provisions about notification in the event of breach.</p>	This is the section that requires the Secretary to amend the existing regulations.
Section 13422 – Regulatory References	References to the C.F.R. refer to provisions in effect on the date of enactment.	No provision.	N/A	N/A



**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**

Section of ARRA	Summary of ARRA Provision	How Addressed under Current Regulations	Significance of Change	Timeline of Required Regulations, if Any
Section 13423 – Effective Date	Except as stated otherwise, provisions shall take effect 12 months after the date of enactment.	No provision.	N/A	N/A
Section 13424 – Studies, Reports, Guidance	<p>(a) Secretary shall prepare and submit reports to Congress concerning alleged violations of law on an annual basis.</p> <p>(b) No later than February 17, 2010, Secretary, in consultation with the FTC, shall conduct study on privacy and security requirements for entities that are not CEs or BAs (including which government agency is best equipped to enforce the requirements) and submit a report to Congress.</p> <p>(c) Secretary shall issue guidance on how to implement requirements for de-identification of PHI (45 C.F.R. § 164.514(b)) within 12 months (no later than February 17, 2010).</p> <p>(d) No later than February 17, 2010, GAO shall submit to Congress a report on best practices related to disclosures for purposes of treatment.</p> <p>(e) Within 5 years (no later than February 17, 2014), GAO shall submit to Congress and the Secretary a report on the impact of any provisions of the Act on health insurance premiums, overall health costs, adoption of EHRs and reduction in medical errors.</p> <p>(f) Secretary shall study definition of psychotherapy notes regarding including test data that is part of mental health evaluation and may issue regulations to refine definition.</p>	No provision.	No likely impact, although guidance issued by Secretary on de-identification of PHI may change de-identification requirements.	New regulations may eventually address changes to definition of psychotherapy notes.

**Ropes & Gray Analysis of HIPAA Provisions under the
American Recovery and Reinvestment Act of 2009 (“ARRA”)**