

# **KUTAK ROCK<sub>LLP</sub>** HEALTH CARE ALERT

March 3, 2009

## **ARRA Amends HIPAA Privacy And Security Provisions**

The following Client Alert addresses the security and privacy provisions for health information contained in The American Recovery and Reinvestment Act of 2009 (“ARRA”), the economic stimulus package enacted into law through signature of President Obama on February 17, 2009. Following are the most critical points for covered entities, business associates and certain other entities:

- While there are provisions with both earlier and later effective dates, ARRA’s provisions are generally effective as of February 17, 2010.
- ARRA imposes new requirements on business associates by recharacterizing them as covered entities.
- ARRA requires modification of contract language in some cases to comply with the requirements prior to the general effective date noted above.
- ARRA significantly enhances the penalties associated with breaches of privacy and security, and it appears that overbroad language contained in business associate agreements not only imposes contractual obligations, but also expands covered entities’ legal obligations. Therefore, covered entities should carefully review business associate agreements and business associate language contained in other contracts to avoid agreeing to overbroad terms.
- ARRA imposes new requirements on certain entities whose business operations involve personal health records.

Other relevant points are discussed in detail in the Client Alert.

### **OVERVIEW**

Titles IV and XIII of ARRA are designed to further the adoption and implementation of health information technology by, among other things: (i) creating a new office within the U.S. Department of Health and Human Services (“HHS”) – the Office of the National Coordinator for Health Information Technology – which will develop, adopt and implement standards, specifications and criteria related to health information technology; (ii) offering hospitals and physicians participating in the Medicare program temporary incentive payments starting in 2011 for using certain electronic health record (“EHR”) technology (and imposing financial penalties beginning in 2015 for failure to use such technology); (iii) offering similar incentives to certain Medicaid providers to assist with the purchase and use of EHR technology; and (iv) providing further protection for the privacy and security of information used and disclosed through such health information technology. According to commentary contained in President Obama’s Budget for Fiscal Year 2010:

These incentives, coupled with other activities authorized in . . . [ARRA], are expected to result in a dramatic increase in the percentage of health care providers using health IT within five years. Computerized health records – while protecting the privacy and security of personal health information – is expected to facilitate improvements in the

quality of health care, prevention of unnecessary health care spending, and a reduction in medical errors.

This Client Alert focuses on the ARRA provisions that relate to protection of the privacy and security of personal health information. ARRA makes changes to a number of the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the regulations promulgated thereunder (the “HIPAA Privacy and Security Provisions”) and regulates entities not previously regulated by the HIPAA Privacy and Security Provisions. More specifically, under ARRA:

- Business associates (“BAs”) are recharacterized as covered entities (“CEs”), requiring BAs to comply with certain provisions of the HIPAA Privacy and Security Provisions;
- BAs and CEs are required to incorporate the changes to the HIPAA Privacy and Security Provisions that have been made by ARRA into their BA agreements;
- The penalty provisions associated with violations of the HIPAA Privacy and Security Provisions are enhanced significantly;
- New notification requirements for breaches of unsecured data are adopted;
- Certain of the current requirements of the HIPAA Privacy and Security Provisions are amended;
- Obligations are imposed on vendors of personal health records (“PHRs”) and certain other related persons not regulated by the HIPAA Privacy and Security Provisions; and
- The way is paved for additional future changes to the HIPAA Privacy and Security Provisions.

Many of these changes will become effective February 17, 2010.

### **PRACTICAL STEPS FOR BAS, CES AND OTHER ENTITIES**

While a more substantive discussion of the privacy and security changes follows, BAs, CEs, PHR vendors and certain related entities will need to take the following steps to ensure compliance with the changes made by ARRA:

- Practical Steps for CEs. A CE should:
  - Inventory and review all provisions of the BA agreements it has entered with BAs, and consider whether the BA agreements need to be amended. A CE should determine whether there is any basis contained in the BA agreement for determining that all of the additional security and privacy requirements are “incorporated” into the BA agreement, without the agreement having to be amended. If BA agreements need to be amended, these amendments must be made by February 17, 2010.
  - Review all of its HIPAA policies and procedures and revise those procedures where necessary to incorporate any new obligations imposed by ARRA.
  - Modify its training programs to include the changes made by ARRA.

- Determine whether it contracts with organizations (i) that provide data transmission of protected health information (“PHI”), and (ii) that require access on a routine basis to such PHI (e.g., Health Information Exchange Organizations, Regional Health Information Organizations, E-prescribing Gateways, or vendors that contract with a CE to allow that CE to offer a PHR to patients as part of its EHR). If it does, then the CE will need to enter into a BA agreement with any such organization.

Note also that, when reviewing and revising these policies and procedures, the CE should also consider whether it is required to comply with the Red Flag Rules adopted by the Federal Trade Commission (“FTC”) and, if it hasn’t already done so, should adopt policies and procedures designed to comply with those rules.<sup>1</sup>

- Practical Steps for BAs. A BA should:

- Inventory and review all provisions of the BA agreements it has entered with CEs, and consider whether the BA agreements need to be amended. BAs should review the BA agreements to:
  - Determine whether there is any basis contained in the BA agreement for determining that all of the additional security and privacy requirements are “incorporated” into the BA agreement, without the agreement having to be amended. If BA agreements need to be amended, these amendments must be made by February 17, 2010.
  - Determine their obligations under the privacy provisions of the BA agreements. Note that ARRA requires BAs to abide by the privacy provisions of the BA agreements and subject BAs to penalties if they do not. Some of the BA agreements may contain provisions greater than those required by the HIPAA Privacy and Security Provisions. If they do, a BA could be held subject to the penalties under HIPAA for a violation of the provisions. If such provisions are contained in the BA agreements, BAs may want to approach the CE and request that these provisions be removed.
- Make sure that it meets the greater administrative, technical and physical safeguard requirements imposed on BAs by ARRA. These requirements are discussed on pages 4 and 5 of this Client Alert.

- Practical Steps for Other Regulated Entities. PHR vendors and certain related entities should:

- Make sure that they have procedures in place to meet the notification requirements imposed by ARRA, as discussed on pages 13 and 14 of this Client Alert.

---

<sup>1</sup> The Red Flag Rules require “creditors” offering or maintaining “covered accounts” to adopt and implement a written identity theft prevention program. The FTC has, through informal statements, taken the position that hospitals and other health care providers are “creditors” with “covered accounts” to the extent they defer payment for services rendered. See the Client Alert at <http://www.kutakrock.com/publications/healthcare/HC092408.pdf> for more information on the FTC’s Red Flag Rules. The Red Flag Rules were originally to be effective on November 1, 2008, but the effective date was subsequently delayed to May 1, 2009.

- Review the guidance released by the Office of Civil Rights (“OCR”) in December 2008 entitled “Personal Health Records and The HIPAA Privacy Rule”<sup>2</sup> to determine the manner in which the HIPAA Privacy and Security Provisions affect the operations of such entities.
- Review the laws of the States in which they operate to make sure their operations are in compliance with the laws of such States.
- Continually monitor proposed regulations and legislation designed to regulate PHR Vendors and related entities and provide appropriate input and comment with respect to such proposed laws.

## **DISCUSSION OF ARRA’S PRIVACY AND SECURITY PROVISIONS**

### **Recharacterization of BAs as CEs**

#### Overview

Currently, the HIPAA Privacy and Security Provisions do not directly regulate BAs, and the penalties associated with a violation of the HIPAA Privacy and Security Provisions may not be imposed directly against a BA. Rather, BAs are only indirectly regulated by the HIPAA Privacy and Security Provisions through contractual obligations with CEs. In the event a CE desires to disclose PHI to a BA or desires a BA to create or receive PHI on its behalf, the HIPAA Privacy and Security Provisions require CEs to obtain certain “satisfactory assurances” from BAs regarding the BA’s use or disclosure of PHI through entering into a written contract or other arrangement with the BA (i.e., a BA agreement). Currently, it is only through these BA agreements that BAs are obligated to abide by certain of the HIPAA Privacy and Security Provisions. Additionally, while a CE might have a breach of contract claim against a BA in the event the BA breached an obligation under the BA agreement, a BA would not currently be subject to any penalties imposed by the government under the HIPAA Privacy and Security Provisions.

ARRA recharacterizes BAs as CEs for purposes of certain of the privacy and security requirements of the HIPAA Privacy and Security Provisions, thereby subjecting BAs to the criminal and civil penalties applicable to CEs for a violation of these provisions.

#### Security Provisions Applicable to BAs

While BAs may have been arguably required to do so previously through provisions in their BA agreements with CEs, ARRA now explicitly requires BAs to adopt the same administrative, technical and physical safeguards as CEs are required to adopt with respect to the electronic PHI (“E-PHI”) that the BA creates, receives, maintains or transmits on behalf of a CE, and subjects BAs to the penalties contained in the HIPAA Privacy and Security Provisions for their failure to do so.

This means that a BA must take the following steps to adopt administrative safeguards applicable to its operations: (i) the BA must identify a security official who is responsible for its security safeguards; (ii) the BA must implement a security awareness and training program for the workforce of the BA; and (iii) the BA must establish and implement policies and procedures that address: (a) preventing, detecting,

---

<sup>2</sup> A copy of this guidance can be found at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf>.

containing and correcting security violations, (b) access to E-PHI by the BA's workforce, (c) detecting, managing and responding to security incidents, and (d) responding to an emergency or other occurrence that damages systems containing copies of E-PHI. BAs must also perform periodic evaluations to ensure that the policies and procedures adopted by a BA continue to meet the administrative safeguard requirements imposed on the BA by the HIPAA Privacy and Security Provisions.

BAs must also establish and implement physical safeguards that: (i) limit physical access to the BA's electronic information systems, ensuring that only properly authorized access is allowed; (ii) address the use of workstations and the accessing of E-PHI at such workstations; and (iii) govern the receipt and removal of hardware and electronic media that contain E-PHI into and out of a facility and the movement of such items within the facility.

Finally, BAs must establish and implement the following technical safeguards: (i) technical policies and procedures that allow access to a BA's electronic information systems that maintain E-PHI only to those persons who have been authorized to access such systems; (ii) software, hardware and/or procedural mechanisms that record and examine activity in information systems containing E-PHI; (iii) policies and procedures to protect E-PHI from improper alteration or destruction; (iv) procedures to verify that a person or entity seeking access to E-PHI is the person or entity he, she or it claims to be; and (v) technical security measures to guard against unauthorized access to E-PHI being transmitted over an electronic communications network.<sup>3</sup>

In addition to implementing the administrative, physical and technical safeguards set forth above, ARRA also provides that any additional requirements imposed by ARRA relating to security that are applicable to CEs are also applicable to BAs.

#### Privacy Provisions Applicable to BAs

Rather than specifying certain sections of the HIPAA Privacy and Security Provisions with which a BA must comply, as it does with respect to the security provisions, in the context of recharacterizing BAs as CEs for purposes of the privacy provisions, ARRA merely provides that a BA may use and disclose PHI only if such use or disclosure is in compliance with the provisions that are included in the BA agreements the BA has entered with CEs. ARRA also provides that any additional privacy requirements imposed by ARRA applicable to CEs are also applicable to BAs.

#### Incorporation of Additional Privacy and Security Requirements into BA agreements

ARRA requires that its additional privacy and security requirements be "incorporated" into the BA agreement between the CE and BA. This seems to require CEs and BAs to amend their current BA agreements to incorporate such requirements, or at least to review their BA agreements to ensure that language in the agreements can be interpreted to "incorporate" such additional requirements.

---

<sup>3</sup> Note also that ARRA request the Secretary to begin issuing annual guidance on the most effective and appropriate technical safeguards.

## New Category of De Facto BAs

Finally, ARRA creates a new de facto category of BAs. Under ARRA, an organization that provides data transmission of PHI to a CE or its BA and that requires access on a routine basis to such PHI is required both to be treated as a BA of such CE and to enter into a BA agreement with the CE.<sup>4</sup>

## **Penalty Provisions**

ARRA explicitly authorizes criminal prosecutions against agents or employees of CEs, increases civil monetary penalty (“CMP”) amounts for HIPAA violations, authorizes individuals to receive a portion of the CMP or settlement amounts received as a result of a HIPAA violation, authorizes State Attorneys General to bring enforcement actions for HIPAA violations, and requires the Secretary of HHS (the “Secretary”) to conduct audits of CEs and BAs. Additionally, any amounts collected will be transferred to OCR to support HIPAA enforcement. These changes increase the risk associated with a violation of the HIPAA Privacy and Security Provisions and will likely lead to greater enforcement actions with respect to such violations.

## Changes to Criminal Penalty Provisions

The Department of Justice released a memorandum in 2005 (the “DOJ Memo”) concluding that HIPAA’s penalty provisions applied only to CEs and that individual employees or agents of a CE would only be subject to criminal prosecution if they could be held directly liable under general principles of corporate criminal liability.<sup>5</sup> The DOJ Memo had the effect of limiting criminal prosecution of such employees and agents, though there have been a few instances of such prosecutions in particularly egregious cases since issuance of the DOJ Memo.

ARRA appears to alter the conclusions of the DOJ Memo by adding language to the criminal penalty provisions of HIPAA that clarifies that a person (including an individual or employee) will now be considered to have obtained or disclosed individually identifiable health information if the information is maintained by a CE and the individual knowingly obtained or disclosed the information without authorization.

## Changes to Civil Penalties

### *Violation Categories and Penalty Tiers*

Violations of the HIPAA Privacy and Security Provisions occurring after February 17, 2009 will be classified into one of four categories, with penalties assessed in accordance with a four-tier system. The category into which a violation falls depends on a determination of the nature and extent of the violation and resulting harm. The four categories of violations are as follows:

- **First Category Violation:** A violation where the person did not know, and by exercising reasonable diligence would not have known, that the person committed a violation is classified as a First Category Violation, subjecting the violator to the First Tier penalties described below.

---

<sup>4</sup> ARRA lists the following as examples of such de facto BAs: Health Information Exchange Organizations, Regional Health Information Organizations, E-prescribing Gateways, or vendors that contract with a CE to allow that CE to offer a PHR to patients as part of its EHR.

<sup>5</sup> A copy of the DOJ Memo may be found at [http://www.usdoj.gov/olc/hipaa\\_final.htm](http://www.usdoj.gov/olc/hipaa_final.htm).

- Second Category Violation: A violation due to reasonable cause and not willful neglect is classified as a Second Category Violation, subjecting the violator to the Second Tier penalties described below.
- Third Category Violation: A violation due to willful neglect that is later corrected is classified as a Third Category Violation, subjecting the violator to the Third Tier penalties described below.
- Fourth Category Violation: A violation due to willful neglect that is not corrected is classified as a Fourth Category Violation, subjecting the violator to the Fourth Tier penalties described below.

The four tier penalty system is as follows, with each tier subject to a cap as outlined below:

- First Tier: \$100 per violation
- Second Tier: \$1,000 per violation
- Third Tier: \$10,000 per violation
- Fourth Tier: \$50,000 per violation

Within each tier, a cap is placed on the penalty that may be assessed per person for repeated violations of an identical requirement or prohibition during a calendar year. While the cap for the First, Second, Third and Fourth Tiers appears to be \$25,000, \$100,000, \$250,000 and \$1,500,000, respectively, ARRA also includes seemingly inconsistent language allowing the First, Second and Third Tier penalties to be capped at \$1,500,000. Due to this inconsistency, the amount of the caps applicable to the First through Third Tiers is not entirely clear.

#### *Willful Neglect Violations*

ARRA imposes new obligations and penalties with respect to HIPAA violations due to willful neglect. ARRA requires the Secretary to formally investigate any complaint of a violation of the HIPAA Privacy and Security Provisions if a preliminary investigation of the facts surrounding the violation indicates that the violation may have resulted from willful neglect. ARRA also requires the Secretary to impose penalties for willful neglect violations, with the amount of those penalties to be within the range set forth in either the Third or Fourth Tier, depending on whether the violation has been corrected. While the mandatory penalty and investigation provisions are not effective until February 17, 2011, it seems that the Secretary would be authorized to impose Third or Fourth Tier penalties on violations occurring after February 17, 2009 that are found to be the result of willful neglect.

#### *Apportionment of Penalties to Individuals*

ARRA authorizes the Secretary to adopt regulations by February 17, 2012 that provide individuals harmed by a violation of the HIPAA Privacy and Security Provisions the ability to recover a portion of the CMPs or settlement payments collected with respect to such a violation. This penalty apportionment methodology will likely incentivize individuals to more actively report violations and lead to increased enforcement activity.

## *Actions by State Attorneys General*

Effective for HIPAA violations occurring on or after February 17, 2009, State Attorneys General are authorized to bring civil actions on behalf of those affected by a HIPAA violation to enjoin further violations by a defendant or to obtain monetary damages. The amount of damages available is determined by multiplying the number of HIPAA violations by up to \$100 per violation, provided that the total amount of damages imposed on a person for all violations of an identical requirement or prohibition during a calendar year may not exceed \$25,000. In the event of a successful action by a State Attorney General, the court may award attorneys' fees and costs to the State, adding to the costs incurred by defendants (i.e., CEs and BAs) as a result of such an action. Additionally, the State is required to provide written notice to the Secretary prior to or upon instituting any such proceeding to permit the Secretary the opportunity to intervene in the matter. These combined enforcement activities could result in significantly greater exposure for CEs, BAs and others regulated by HIPAA.

### Auditing of CEs and BAs

Under current law, the Secretary is authorized to conduct compliance reviews to determine whether CEs are complying with HIPAA standards. ARRA requires the Secretary to perform periodic audits to ensure that CEs and BAs are meeting the HIPAA Privacy and Security Provisions, as amended by ARRA and its implementing regulations. These modifications are effective February 17, 2010.

## **Notification of Unsecured PHI Breaches**

### CE Obligations

If a CE discovers<sup>6</sup> a breach (defined below) of unsecured PHI<sup>7</sup> and if, as a result of the breach, the unsecured PHI of an individual has been, or is reasonably believed by the CE to have been, accessed, acquired or disclosed, ARRA requires the CE to make the following notifications:

- The CE must provide notice to the individual (or next of kin if the individual is deceased). The notice must be provided promptly via written notification at the last known address of the individual or next of kin, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available. A substitute form of notice is available in the event there is insufficient or out-of-date contact information for the individual. Additionally, if a CE determines that there is possible imminent misuse of unsecured PHI, the CE may provide information to individuals by telephone or other means, in addition to the written notification.

---

<sup>6</sup> A breach is treated as "discovered" by a CE or a BA as of the first day on which such breach is known to the CE or BA (including any person, other than the individual committing the breach, that is an employee, officer or other agent of the CE or BA) or would reasonably have been known to such CE or BA (or person) to have occurred.

<sup>7</sup> The term "unsecured PHI" is defined as PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance to be issued within sixty (60) days after February 17, 2009. This guidance will specify the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals. In the event the Secretary does not render guidance by the date specified above, the term "unsecured PHI" means PHI not secured by a technology standard that renders PHI unusable, unreadable or indecipherable to unauthorized individuals and is developed or endorsed by a standards development organization accredited by the American National Standards Institute.

Any notice to an individual is required to include (i) a brief description of the event (including the date of the breach and the date of the discovery of the breach, if known), (ii) a description of the types of information involved in the breach (e.g., full name, SSN, date of birth, home address, account number, or disability code), (iii) the steps individuals should take to protect themselves from potential harm resulting from the breach, (iv) a brief description of the steps the CE is taking to investigate the breach, to mitigate losses, and to protect against further breaches, and (v) contact procedures for individuals to ask questions or learn additional information, which must include a toll-free number, an email address, a Web site or a postal address.

- The CE must provide notice to prominent media outlets serving a State or jurisdiction, if the breach involves more than 500 residents of such State or jurisdiction.
- The CE must provide notice to the Secretary. The form of notice depends on the number of individuals affected by the breach. If the breach occurred with respect to 500 or more individuals, notice to the Secretary must be given immediately. If fewer than 500 individuals, the CE is allowed to maintain an annual log of the occurrence of any such breach and submit the log to the Secretary annually. Note that the Secretary is required to post on the HHS web site a list identifying each CE involved in a breach in which the unsecured PHI of more than 500 individuals is acquired or disclosed.

A “breach” occurs under ARRA upon the occurrence of an unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI, unless an unauthorized person to whom the PHI is disclosed would not reasonably have been able to retain the PHI. In addition, an unintentional acquisition, access or use of PHI by an employee or individual acting under the authority of a CE or BA is not considered to be a “breach” if (i) the acquisition, access or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual with the CE or BA and the PHI is not further acquired, accessed, used or disclosed by any person, and (ii) if the acquisition, access or use is an inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a CE or BA to another similarly situated individual at the same facility and if the PHI received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person.

#### BA Obligations

Similarly, ARRA requires BAs who discover a breach of unsecured PHI to notify the CE of such breach. The BA’s notice must identify each individual whose unsecured PHI has been, or is reasonably believed by the BA to have been, accessed, acquired or disclosed during the breach.

#### Timing of Notice

Except in situations where law enforcement determines that a notification, notice or posting required by ARRA would impede a criminal investigation or cause damage to national security, CEs and BAs must provide the notice(s) required by ARRA without delay and in no case later than sixty (60) calendar days after the discovery of the breach.

#### Effective Date of Notification Requirement

The Secretary is required to promulgate interim final regulations not later than the date that is 180 days after February 17, 2009. The notification requirements with respect to unsecured PHI apply to breaches

that are discovered on or after the date that is thirty (30) days after the date of publication of such interim final regulations.

### State Obligations

ARRA incorporates HIPAA's state preemption analysis to ARRA's provisions. Therefore, certain State laws, including those "more stringent than" the ARRA provisions, will not be preempted by ARRA. Many States have enacted identity theft laws that encompass the theft or unauthorized access of medical information. CEs, BAs, and others regulated by these laws will need to continue to comply with these laws, to the extent these laws are not preempted by ARRA.

### **Other ARRA Changes Relating to Privacy and Security**

#### Prohibition on the sale of PHI

ARRA imposes a new requirement on CEs and BAs that prohibits CEs and BAs from directly or indirectly receiving remuneration in exchange for any PHI of an individual unless:

- the CE obtains a valid authorization from the individual that specifies whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that individual;
- the exchange is for public health activities;
- the exchange is for research, and the price charged reflects the costs of preparation and transmittal of the data for research purposes;
- the exchange is for treatment of the individual, subject to any regulation adopted by the Secretary to prevent PHI from inappropriate access, use or disclosure;
- the exchange is for the sale, transfer, merger, or consolidation of all or part of the CE with another CE, or an entity that following such activity will become a CE and due diligence related to such activity;
- the exchange is for remuneration that is provided by a CE to a BA for activities involving the exchange of PHI that the BA undertakes on behalf of and at the specific request of the CE pursuant to a BA agreement;
- the exchange is to provide an individual with a copy of his or her PHI; or
- the exchange is for a purpose set forth in regulations to be adopted by the Secretary.

Note that these exceptions do not directly address all situations in which the sale of medical records takes place. For example, the exceptions do not directly address the sale of a hospital's medical records to a previously employed physician in the event the hospital ceases to employ the physician. Although a case may be made that such a sale falls within the individual treatment exception, CEs will want to review the above exceptions and provide comment to the regulations that are to be adopted by the Secretary to ensure that common situations in which medical records or PHI is sold to a third party are addressed in the regulations.

This prohibition is effective on the date that is six (6) months after the date of adoption of the Secretary's regulations addressing this prohibition. These regulations are to be adopted not later than eighteen (18) months after February 17, 2009.

#### Accounting of Certain PHI Disclosures

The HIPAA Privacy and Security Provisions generally require CEs to provide individuals an accounting of the disclosures made by a CE for a period of six (6) years prior to the date of an individual's request of the accounting. Certain disclosures, including disclosures made for carrying out treatment, payment and health care operations, are not currently subject to this accounting requirement.

ARRA amends the treatment, payment and health care operations exception to the accounting requirement. Under ARRA, CEs that use or maintain an EHR<sup>8</sup> will be required to provide individuals with an accounting of the disclosures of PHI made to carry out treatment, payment and health care operations when the disclosures were made through an EHR for a period of three (3) years prior to the date of an individual's accounting request.<sup>9</sup>

If the CE has BAs making disclosures of PHI for treatment, payment or health care operations through an EHR, the CE must either include those disclosures in its accounting or must provide a list of all BAs that act on behalf of the CE, including the contact information for such BAs (e.g., mailing address, phone and email address). The BAs included on the list must provide an accounting of disclosures made by the BA upon a request made by an individual directly to the BA for such an accounting.

The date on which CEs and BAs are required to abide by these new accounting requirements depends on the date the CE acquires an EHR. If such acquisition had taken place as of January 1, 2009, then the requirements apply to disclosures of PHI made through such EHRs on or after January 1, 2014. If a CE acquired an EHR after January 1, 2009 but prior to January 1, 2011, the new accounting requirements will apply to disclosures of PHI made through such EHRs on or after January 1, 2011. Finally, if a CE acquired an EHR after January 1, 2011, the new accounting requirements will apply to disclosures of PHI made through such EHRs on or after the date of acquisition of the EHR. Subject to certain restrictions, the Secretary may delay any of the dates set forth above.

#### Modification of an Individual's Right to Access PHI

Currently, subject to certain exceptions, the HIPAA Privacy and Security Provisions provide individuals with a right of access to inspect and obtain a copy of their PHI. ARRA expands these rights. Under ARRA, individuals have the right to obtain from a CE who uses or maintains an EHR a copy of the PHI in an electronic format and, if the individual chooses, to direct the CE to transmit such copy directly to an entity or person designated by the individual, provided the choice is clear, conspicuous and specific. While a CE may charge a fee to an individual for obtaining a copy of his or her PHI in an electronic form, the fee is limited to the CE's labor costs in responding to the request for the copy. These modifications are effective February 17, 2010.

---

<sup>8</sup> The term "EHR" or "electronic health record" is defined as an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

<sup>9</sup> The Secretary is required to adopt regulations that provide further information of the requirements of such accounting of disclosures of PHI made through an EHR.

## CEs Required to Agree to Certain Restrictions on PHI Disclosures

Currently, the HIPAA Privacy and Security Provisions allow an individual to request that a CE limit certain uses or disclosures of PHI, but a CE is not required to agree to such a requested restriction. ARRA changes that. Under ARRA, the CE must agree to a requested restriction if (i) the request is to limit the disclosure to a health plan for purposes of carrying out payment or health care operations (i.e., the request is not to limit disclosures for the purpose of carrying out treatment) and (ii) the PHI that is the subject of the request pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full. This change appears to be designed to allow patients to prohibit their providers from telling insurance companies about their treatment as long as the patients pay in full for that treatment. These modifications are effective February 17, 2010.

## Changes to Marketing Rules

Currently, CEs may not engage in marketing activities involving the use and disclosure of an individual's PHI without an authorization, but there is an exception that allows CEs (or their BAs) to encourage patients to purchase or use a health care-related product or service without an authorization, even if the CE is paid by a third party to engage in such activities. ARRA places further restrictions on these excepted communications.

Under ARRA, CEs and BAs may continue to engage in communications about a product or service that encourage recipients of the communication to purchase or use the product or service without obtaining an authorization, as long as the communications (i) describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the CE making the communication, (ii) relate to treatment of the individual, or (iii) relate either to case management or care coordination for the individual, or to the recommendation of alternative therapies, treatments, health care providers or settings of care for the individual. ARRA continues to allow CEs to receive direct or indirect payment in exchange for these communications but only if the communication relates to a drug or biologic that the patient is currently prescribed, the payment amount is reasonable, and certain other conditions are met.<sup>10</sup> These changes are effective February 17, 2010.

## Enhanced Restrictions When Disclosing PHI

Currently, when using or disclosing PHI or when requesting PHI from another CE, the HIPAA Privacy and Security Provisions require a CE to use reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purposes of the use, disclosure or request. Currently, the minimum necessary requirement is subject to certain exceptions.

ARRA requires the Secretary to issue guidance on the minimum necessary requirement not later than eighteen (18) months after February 17, 2009. Until the Secretary issues this guidance, CEs, and BAs acting on behalf of CEs, are required to limit the use, disclosure or request of PHI, to the extent practicable, to the limited data set<sup>11</sup> or if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure or request, respectively. The new limited data set/minimum

---

<sup>10</sup> ARRA further requires the Secretary to adopt regulations that allow recipients of written fundraising communications to elect not to receive any further such communications and requires that any such election be treated as a revocation of an authorization previously provided by the individual.

<sup>11</sup> Note that a limited data set, while not meeting the definition of de-identified information, has most direct identifiers removed and is considered by HHS to pose a low privacy risk.

necessary requirement continues to be subject to the same exceptions currently provided for the minimum necessary requirement.

### **Notification Obligations Related To PHRs<sup>12</sup>**

ARRA imposes three separate notification requirements relating to PHRs.

First, ARRA requires non-CE entities that offer or maintain PHRs (“PHR Vendors”) to notify the following persons after discovery of a breach of security<sup>13</sup> of unsecured<sup>14</sup> PHR identifiable health information that is in a PHR maintained or offered by the PHR Vendor:

- Each individual who is a U.S. citizen or resident whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security, and
- The FTC, which is required subsequently to notify the Secretary.

Second, ARRA requires Related PHR Entities, defined below, to make the same notifications as PHR Vendors after discovery of a breach of security of unsecured PHR identifiable health information that is obtained through a product or service provided by such Related PHR Entity. “Related PHR Entities” are (i) entities that offer products or services through the website of PHR Vendors, (ii) non-CE entities that offer products or services through the website of CEs that offer individuals PHRs, and (iii) non-CE entities that access information in a PHR or send information to a PHR.

Third, ARRA requires a third party service provider that provides services to a PHR Vendor or to a Related PHR Entity in connection with the offering or maintenance of a PHR or a related product or service and that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured PHR identifiable health information in such a record as a result of such services, following the discovery of a breach of security of such information, to notify the PHR Vendor or Related PHR Entity of such breach. This notice must include the identification of each individual whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, accessed, acquired or disclosed during such breach.

The timing, method and content of notifications required with respect to PHR Vendors, Related PHR Entities or third party service providers are the same as those set forth with respect to breaches of unsecured PHI. Violations of these notification requirements is treated as an unfair and deceptive act or

---

<sup>12</sup> A “PHR” or “personal health record” is defined 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. The term “PHR identifiable health information” is defined as individually identifiable health information that (i) is provided by or on behalf of an individual and (ii) identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

<sup>13</sup> The term “breach of security” means acquisition of the unsecured PHR identifiable health information of an individual in a PHR without the authorization of the individual.

<sup>14</sup> The term “unsecured PHR identifiable health information” means PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary in the guidance described in note 7. In the event the Secretary does not issue such guidance by the date specified in note 7, the term “unsecured PHR identifiable health information” means PHR identifiable health information that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals and that is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

practice and presumably subject the violators to the penalties associated with an unfair and deceptive act or practice.

The FTC is required to promulgate interim final regulations by a date not later than 180 days after February 17, 2009. The PHR notification provisions apply to breaches of security that are discovered on or after the date that is thirty (30) days after the date of publication of such interim final regulations.

### **Additional Potential Future Changes**

ARRA authorizes a number of reports and studies by various agencies, including, without limitation, (i) an annual report prepared by the Secretary of complaints received by the Secretary with respect to alleged violations of law relating to the privacy and security of health information and (ii) a study and report to certain agencies by the Secretary, in consultation with the FTC, on privacy and security requirements for entities that are not CEs or BAs as of February 17, 2009.

Clearly, from the studies and reports authorized by ARRA, regulation of CEs, BAs, PHR Vendors, and other entities with respect to the privacy and security of health information will be a moving target, with a high potential of further regulations and requirements in the coming years. CEs, BAs, PHR Vendors and Related PHR Entities should keep this in mind when drafting policies and procedures and taking the other steps necessary to comply with these provisions.

### **FIRM CONTACT INFORMATION**

We hope this Client Alert has been helpful to you. For more information regarding ARRA's changes to the HIPAA Privacy and Security Provisions or how your organization should proceed in light of these changes, or if you have any other questions regarding this Client Alert, please feel free to contact any of the following, or your regular Kutak Rock LLP contact or any member of our Health Care Practice group:

Melany C. Birdsong  
[Melany.Birdsong@KutakRock.com](mailto:Melany.Birdsong@KutakRock.com)  
(501) 975-3000

Bryan G. Looney  
[Bryan.Looney@KutakRock.com](mailto:Bryan.Looney@KutakRock.com)  
(479) 973-4200

Chris Phillips  
[Chris.Phillips@KutakRock.com](mailto:Chris.Phillips@KutakRock.com)  
(402) 346-6000

Mark L. Sabey  
[Mark.Sabey@KutakRock.com](mailto:Mark.Sabey@KutakRock.com)  
(303) 297-2400

G. Mark Sappington  
[Mark.Sappington@KutakRock.com](mailto:Mark.Sappington@KutakRock.com)  
(816) 960-0090

Heather Schmiegelow  
[Heather.Schmiegelow@KutakRock.com](mailto:Heather.Schmiegelow@KutakRock.com)  
(479) 973-4200