CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Summary of Health Privacy Provisions in the 2009 Economic Stimulus Legislation

April 29, 2009*

The American Recovery and Reinvestment Act of 2009 (ARRA, sometimes referred to as "the stimulus") included provisions making significant improvement in the privacy and security standards for health information. The provisions on privacy and security (generally in ARRA's Title XIII, Subtitle D and some parts of Subtitle A) can be grouped into four broad categories:

- Substantive changes to HIPAA statute and privacy and security regulations
- Changes in HIPAA enforcement
- Provisions to address health information held by entities not covered by HIPAA (as either covered entities or business associates)
- Miscellaneous: Administration/Studies/Reports/Educational Initiatives

For each set of changes, this summary indicates when the provision goes into effect and whether the Secretary is required to promulgate regulations or guidance or adopt technical standards. Appendix A also sets forth an overall calendar with effective dates for various provisions and due dates for reports, regulations and standards related to privacy.

Substantive Changes to HIPAA Statute & Regulations

Changes in How Business Associates Must Comply with HIPAA and Clarification of Who Is a Business Associate

Before ARRA, HIPAA required that covered entities such as hospitals, physicians and health plans had to enter into contracts (known as "business associate agreements")

* The original version of this summary was dated March 12, 2009. The first edited version, dated March 24, 2009, contained minor edits but no substantive changes with respect to the legal analysis of the ARRA provisions. This third version, dated April 29, 2009, reflects only changes to effective dates that were incorrectly stated in the March 24, 2009 version.

with entities performing functions or providing services on their behalf (where those functions or services involved the exchange of health information). The contracts had to require the business associates to use appropriate security safeguards to protect the health information they received from the covered entity. The business associate agreements also set forth the permitted uses and disclosures of such health information. However, prior to ARRA, business associates were not directly subject to governmental enforcement action: the only remedy available against a business associate was for a covered entity to sue for breach of contract.

Under Section 13401 of ARRA, business associates are required to directly comply with most provisions of the HIPAA Security Rule.[1] With respect to compliance with the Privacy Rule, under Section 13404 of ARRA, business associates must comply with those Privacy Rule provisions that are made applicable to them by their contract with the covered entity; they also must comply with any changes to the Privacy Rule that were part of ARRA regardless of whether or not those provisions are in their contracts with covered entities.[2] As noted below in the enforcement section, business associates can now be held directly accountable by federal or state authorities for any failure to comply with HIPAA as amended by ARRA or applicable regulations.

Section 13408 of ARRA also clarifies that entities that transmit or process data on behalf of covered entities, like Regional Health Information Organizations (RHIOs), Health Information Exchanges (HIEs) or E-Prescribing Gateways, are business associates for purposes of HIPAA. A vendor that "contracts with a covered entity to allow that covered entity to offer a personal health record to patients as a part of its electronic health record" also is also required to enter into a business associate agreement.[3] Some PHR vendors have argued that the provision does not apply to them, even when they contract with a covered entity, because the PHR being offered remains the PHR of the vendor and is not "part of the electronic health record" of the covered entity. CDT agrees, and interprets this provision to cover only those circumstances where a PHR vendor is contracting with a covered entity so that the covered entity can offer its own PHR to its patients. (For example, PHR vendor

---

[1] Sections 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies and procedures and documentation requirements) of title 45, Code of Federal Regulations.

[2] ARRA states that the Privacy Rule changes "shall be incorporated" into business associate agreements (Section 13404); it is not clear whether business associate agreements need to be renegotiated to include these provisions or whether they are now incorporated into such agreements as a matter of law.

[3] Note that HHS issued HIPAA guidance in December 2008 stating that health information exchanges transmitting data on behalf of covered entities would need to be business associates, and that personal health records offered by covered entities would be covered by the Privacy Rule.

contracting with Smithville Hospital so that a Smithville Hospital PHR can be offered to patients.)

Regulations/Standards: None required.
Effective Date: February 18, 2010.

Breach Notification

Prior to ARRA, HIPAA did not require covered entities to notify individuals of breaches of their protected health information. ARRA Section 13402 requires that covered entities provide notification to individuals if their health information has been breached (business associates are required to notify covered entities of any breaches; the covered entity must then notify the individual per the requirements). In determining whether or not notice is required, two questions are relevant: (1) did it qualify as "breach" under the breach definition, and (2) was the information protected by an encryption-like technology. Even if the access or release of information qualifies as a breach, individuals are not required to be notified if the information was protected by a technology approved by the Secretary.

Breach is defined as the unauthorized acquisition, access, use or disclosure of protected health information – but there are a number of exceptions. It is not a breach:

- Where an unauthorized person who receives the health information cannot reasonably have been able to retain it;

- If an unintentional acquisition, access or use occurs within the scope of employment or a professional relationship and the information does not go any further (i.e., it is not further acquired, accessed, used or disclosed); or

- If it is an inadvertent disclosure that occurs within a facility, and the information does not go any further.

Only breaches of "unsecured" health information trigger the notification requirement. Similar to California law, which does not require notification if the information is encrypted (as long as the encryption has not been compromised), a breach of information that has been rendered "unusable, unreadable or indecipherable to unauthorized individuals," using a technology or methodology specified by the Secretary, does not trigger the notification requirement. The Secretary is directed to consult with stakeholders and issue guidance, within 60 days of ARRA enactment, specifying a list of technologies and methodologies that meet this standard. (Note that this list must be updated on an annual basis.) If the breach notification requirement goes into effect and the Secretary has not yet issued guidance, information that is protected by technology that renders information unusable, unreadable or indecipherable and that is developed and endorsed by a

standards developing organization accredited by ANSI will qualify for this "safe harbor."

ARRA includes specific provisions regarding the content, methods and timing of notification. Notice must be afforded no later than 60 days after the discovery of the breach. A breach is considered to be "discovered" when at least one employee of the entity (other than the person responsible for the breach) knows (or reasonably should know) of the breach. Notice is required to be provided to media outlets if the information of more than 500 individuals is involved. Notice of all breaches also must be provided to the Secretary (immediately if the breach involves the information of more than 500 individuals and in an annual log for breaches that do not trigger this threshold). The Secretary is required to include a list on the HHS website of covered entities involved in breaches of more than 500 individuals' information, and must annually report to Congress on the number and nature of any breaches that occurred during that year.

These breach provisions do not expressly preempt any applicable state breach notification laws. Failure to notify constitutes a violation of HIPAA (Section 13410(a)(2)).

> **Regulations/Standards:** Within 60 days of enactment, the Secretary must specify the technologies that render data unusable or unreadable. By August 18, 2009, the Secretary is required to promulgate interim final regulations to implement the breach notification requirements.
> **Effective Date:** Applies to breaches that are discovered on or after 30 days after interim final regulations are promulgated (September 18, 2009).

<u>Strengthened Right to Restrict Disclosures</u>

Currently under HIPAA, individuals have the right to request a restriction on certain uses and disclosures of their protected health information, but covered entities are under no obligation to comply with that request. Section 13405(a) of ARRA requires covered entities (and their business associates) to honor an individual's request to restrict disclosure of protected health information to a health plan for purposes of payment or health care operations if the information pertains *solely* to a health care item or service that the individual has paid for in full out-of-pocket.

> **Regulations/Standards:** None required.
> **Effective Date:** February 18, 2010.

<u>Guidance on Minimum Necessary/Interim Deeming of Limited Data Set as Sufficient</u>

Under the Privacy Rule, covered entities are required, except in cases of treatment and certain other purposes, to access, use and disclose only the *minimum necessary* amount of protected health information needed to satisfy the purpose for which the data was acquired, used or disclosed. A covered entity may rely on the entity

requesting the data in determining what constitutes minimum necessary, if it is reasonable to do so (and if the data is requested by another covered entity, by a public official in certain circumstances, or by a professional member of its workforce or one of its business associates). The Privacy Rule also provides for a limited data set, which is stripped of a number of categories of patient identifying information and can be used pursuant to a data use agreement for research, public health and health care operations purposes.

Under Section 13405(b) of ARRA, the Secretary is required to establish guidance on what constitutes minimum necessary, which CDT hopes will provide covered entities more clarity regarding the steps they should take to comply with the standard. CDT is urging the Secretary to consider as well whether there are some purposes for which identified data is permitted to be used under the current standard but which in fact should be required to use a limited data set or some other form of anonymized data. ARRA also provides that the data holder must not rely solely on the judgment of the data requester but must determine for itself what constitutes the minimum amount of information needed. There was no change to scope of uses and disclosures covered by the minimum necessary standard.

Until the Secretary issues this guidance, covered entities should use a limited data set to meet the minimum necessary standard – but only if such use is practicable. Entities may still rely on the flexible minimum necessary standard in lieu of the limited data set if they need to in order to accomplish the intended purpose of accessing, using or disclosing the information.

> **Regulations/Standards:** Guidance (not regulations) must be issued within 18 months of enactment.
> **Effective Date:** The provision on using limited data sets to satisfy the minimum necessary standard goes into effect on February 18, 2010 and remains in effect until the guidance is issued.

Accounting for Disclosures

The ARRA changes the requirements for generating an accounting of disclosures per patient request for covered entities using electronic health records (which is a defined term in the statute).[4] Under the current Privacy Rule, covered entities must provide to an individual, upon request, an accounting of disclosures of protected health information made from the individual's medical record for the previous six years – but a number of disclosures are specifically exempted from this requirement, including disclosures for treatment, payment, and health care

[4] 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." Section 13400.

operations. The accounting provided by a covered entity must also include any applicable disclosures by the entity's business associates.

Under Section 13405(c) of ARRA, covered entities using electronic health records may no longer exempt disclosures for treatment, payment and health care operations, although the accounting need only cover the previous three years. The Secretary is required to promulgate regulations to define what needs to be collected about each disclosure, taking into consideration what patients have an interest in learning about disclosures from their records and the administrative burden on the covered entity. Covered entities may include disclosures from business associates in the accounting report they develop for patients, or they can give patients a list of the business associates involved in disclosing protected health information from their records (and contact information) and direct patients to request an accounting directly from the business associate. The business associate must comply with such a request.

> **Regulations/Standards:** The Secretary is required to adopt a technical standard to enable EHRs to produce an accounting for disclosures for treatment, payment and health care operations (and such standard must be among those adopted in the initial prioritized set of standards, which must occur no later than 12/31/2009); regulations must be promulgated no later than six months after the adoption of the relevant technical standards.
>
> **Effective Date:** For entities adopting electronic health records by January 1, 2009, the new provisions apply on January 1, 2014 (which the Secretary can extend if necessary until 2016), and for those adopting electronic records on or after 1/1/2009, the new provisions apply on the later of the date the record is acquired or January 1, 2011 (which the Secretary can extend if necessary to 2013).

<u>Prohibition on "Sale" of Protected Health Information</u>

Section 13405(d) of ARRA prohibits the direct or indirect receipt of remuneration in exchange for an individual's protected health information without an authorization from that individual (which must also specify whether the information can be further exchanged for remuneration by the entity initially receiving the data). There are several exceptions to this provision:

- For public health activities described in the Privacy Rule;
- For research (as described in the Privacy Rule), as long as the price charged reflects the costs of preparation and transmittal of the data;
- For treatment of the individual, subject to any regulations the Secretary may promulgate to prevent inappropriate use of the data;
- When the covered entity is being sold, transferred, merged or consolidated (in whole or in part) with another covered entity (or an entity that will

become a covered entity after the transaction), and any due diligence associated therewith;
- When the remuneration is provided by a covered entity to a business associate for activities that the business associate is undertaking on behalf of and at the specific request of the covered entity;
- To provide an individual with a copy of his or her protected health information;
- Any other exception determined by the Secretary in regulation to be similarly necessary and appropriate as the foregoing exceptions.

Regulations/Standards: Not later than August 18, 2010, the Secretary must promulgate regulations to carry out these provisions. In the regulations, the Secretary must evaluate the impact on research or public health activities, including any conducted by the FDA, of restricting remuneration for data disclosed for public health purposes to the costs of preparing and transmitting the data. The Secretary may impose such a restriction if he or she finds that it will not impede such research or public health activities. As noted above, the Secretary also may impose further regulations on the treatment exception to prevent inappropriate access, use or disclosure of data.

Effective Date: Six months after the promulgation of final regulations.

Individual Right of Electronic Access

Under the Privacy Rule, individuals have always had a right to access and obtain a copy of their health records "in the form or format requested" – if it is "readily producible" in such form or format – within 30 days of the request in most circumstances. The covered entity may impose a "reasonable fee" for such access or copy; any limits on such charges are usually governed by state law.

Under Section 13405(e) of ARRA, covered entities using electronic health records must provide individuals with an electronic copy of the record, which must be transmitted directly to an entity or person specified by the individual, as long as that directive is clear, conspicuous and specific.[5] Any fee charged for the record cannot be greater than the entity's labor costs in responding to the request. The ARRA provisions do not change the timeframe for responding to requests for record copies.

Regulations/Standards: None required.

[5] Note that the right to an electronic copy is to information in the "electronic health record," as defined in the legislation. Under the Privacy Rule, a patient's right of access is only to protected health information in a designated record set.

Effective Date: February 18, 2010.

When Authorization is Required for Marketing Communications

Under the HIPAA Privacy Rule, covered entities have been required to obtain authorization from an individual before using his or her protected health information for marketing purposes. The definition of marketing in the Rule includes a number of exceptions. In summary, until ARRA takes effect, covered entities do not need prior authorization to use information to send communications that: (i) describe products or services offered as part of a health benefits plan or that are "value-added" services available to plan enrollees; (ii) are for treatment of the individual; or (iii) are for case management or care coordination or direct patients to alternative treatments, therapies, providers or settings of care.[6]

The Rule also prohibits covered entities from selling protected health information to outside entities for the purpose of marketing. However, outside entities can pay covered entities to send marketing communications to patients and no authorization is required, as long as the communication is of a type that meets one of the exceptions.

Under Section 13406(a) of ARRA, if a covered entity is paid by an outside entity to send a communication to a patient, the communication is deemed to be marketing and requires prior authorization from the patient – even if that communication falls into one of the current exceptions to the definition. However, there are exceptions to this new rule. Protected health information may be used without authorization for communications that describe a drug or biologic that is currently being prescribed for or administered to the person, as long as the payment received by the covered entity is "reasonable in amount" (which the Secretary must determine by regulation). ARRA also makes clear that communications that have the patient's authorization may be "sponsored" by outside entities. The ARRA provision also clarifies that the prohibition on receipt of remuneration does not apply to compensation paid by a covered entity to a business associate to make a communication on its behalf (as long as the communication is sent consistent with the business associate agreement).

The provision also makes clear that the term "direct or indirect remuneration" does not include any payment for treatment of an individual.

Regulations/Standard: The Secretary is not specifically directed to promulgate regulations, but the meaning of what constitutes payment that is "reasonable in amount" is to be set by the Secretary in regulation.
Effective Date: February 18, 2010. (Not tied to promulgation of regulations)

[6] 45 C.F.R. 164.501.

Opt-out for Fundraising Communications

Under the Privacy Rule, covered entities have been able to use an individual's demographic information and the dates that any health care was provided to an individual to send fundraising communications to the individual without first obtaining the individual's authorization. Such communications must include a description of how a person can opt-out of receiving further communications, and entities must make reasonable efforts to comply with any opt-out requests.

Section 13406(b) of ARRA requires the Secretary to promulgate a rule requiring that the opportunity to opt-out of receiving fundraising communications be presented to the recipient in a clear and conspicuous manner.

> **Regulations/Standards:** The Secretary is required to establish this provision by rule.
> **Effective Date:** Applies to communications occurring on or after February 18, 2010. (Note: Unclear what happens if the Secretary does not issue a rule implementing this provision).

Changes to HIPAA Enforcement

The ARRA includes a number of changes to HIPAA's enforcement provisions:

- Direct Accountability for Business Associates. Sections 13401 and 13404 of ARRA provide that business associates can be held accountable by federal and state authorities for failure to comply with any applicable provisions of the Privacy and Security Rules. Under current regulations, government authorities cannot hold business associates accountable for failing to comply with their business associate agreements, and covered entities can only be held liable for the actions of their business associates in limited circumstances.

  Regulations/Standards: None required.
  Effective Date: February 18, 2010.

- Application of Criminal Penalties. Section 13409 of ARRA clarifies that HIPAA's criminal penalties can be enforced against individuals, including (but not limited to) employees of a covered entity. This overrules a Department of Justice Office of Legal Counsel memo issued during the Bush Administration that stated that only covered entities could be criminally prosecuted for violations of HIPAA. In addition, the wording of the provision may broaden the scope of activities for which criminal penalties can be attached because authorities can prosecute an individual who obtains or

discloses individually identifiable health information "without authorization."

Regulations/Standards: None required.
Effective Date: February 18, 2010.

- Clarification of When Civil Penalties Can (or Must) Be Pursued. Section 13410(a) of ARRA clarifies that HHS and state attorneys general can pursue a civil HIPAA violation in cases where criminal penalties could attach but the Department of Justice declines to pursue the case. This Section requires that the Secretary formally investigate any complaint where a preliminary investigation of the facts indicates a possible violation due to willful neglect. It also requires the Secretary to impose a civil monetary penalty if a violation is found to constitute willful neglect of the law. The Bush Administration interpreted the current HIPAA statute and regulations as providing it the discretion to resolve most HIPAA complaints informally.

  Regulations/Standards: Must be promulgated by the Secretary no later than August 18, 2010.
  Effective Date: applies to penalties imposed on or after February 18, 2011.

- Distribution of Civil Monetary Penalties. Section 13410(c) of ARRA requires that any civil monetary penalties or settlements collected for HIPAA violations must be transferred to the HHS Office of Civil Rights to be used for enforcement purposes. (Currently, any civil penalties or settlements go to the general treasury.) GAO is required to develop a methodology for individuals who are harmed by HIPAA violations to receive a percentage of any penalty or monetary settlement collected, and the Secretary must establish such a methodology by regulation within three years of enactment.

  Regulations/Standards: GAO report is due August 17, 2010; Secretary's regulations on the methodology for compensating individuals for harm must be established by February 18, 2012.
  Effective Date: Penalties and settlements go to OCR effective February 18, 2010. The new methodology applies on or after the effective date of the regulation.

- Tiered Increase in Civil Monetary Penalties. The current HIPAA statute sets civil penalties at $100 per violation, with an annual maximum of $25,000 for violations of the same requirement. Section 13410(d) of ARRA sets a new tiered penalty structure, based on the level of the HIPAA violation, which tops out at $50,000 per violation and an annual maximum of $1.5 million. (See civil penalty chart at Appendix B.) The Secretary still has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm. The Secretary is also precluded from imposing civil penalties (except in cases of willful neglect) if

the violation is corrected within 30 days (a time period which may be extended).

Regulations/Standards: None required.
Effective Date: Applies to violations occurring after February 17, 2009.

- Authorization for State Attorneys General Enforcement. A handful of states authorize their attorneys general to enforce federal consumer protection laws (including HIPAA). Section 13410(e) of ARRA expressly authorizes all state attorneys general to enforce HIPAA in federal district court, which means that attorneys general in all states can enforce the law even if there is no state authorizing statute. The state must serve notice upon the Secretary of any intent to enforce the law, and the Secretary has the right to intervene in the action. The penalties imposed are limited to the former statutory maximum: $100 per violation and $25,000 annually for repeat violations of the same provision.

  Regulations/Standards: None required.
  Effective Date: Applies to violations occurring after February 17, 2009.

- Secretary's Audit Authority. Currently HHS has authority to audit entities for compliance with both the Privacy and Security Rules. Section 13411 of ARRA makes it clear that the Secretary must do periodic audits to ensure compliance with these Rules.

  Regulations/Standards: None required.
  Effective Date: February 18, 2010.

Provisions for Entities Not Covered by HIPAA (either as covered entities or business associates)

Breach Notification Requirements

Section 13407 of ARRA establishes breach notification requirements for vendors of personal health records and other non-HIPAA covered entities. A 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." (Section 13400) "PHR identifiable health information" includes individually identifiable health information, as defined in HIPAA (which includes personal health information from a covered entity), as well as information provided by or on behalf of the individual and that identifies the person (or with respect to which there is a reasonable basis to believe the information can be used to identify the individual). (Section 13407) CDT believes this covers the consumer-facing health record tools currently being offered by non-

HIPAA covered entities to the public (or by employers to employees), including health record banks.

The breach notification requirements apply also to:

- Entities that offer products or services through the website of a vendor of personal health records;
- Entities that are not themselves HIPAA-covered entities but that offer products or services through the websites of covered entities with PHRs;
- Entities that are not themselves HIPAA-covered entities and access information in, or send information to, a PHR.

In the event of a breach, these entities must directly notify the individuals involved. Third party entities that provide services to the PHR vendor and the foregoing categories of entities must notify the entity with which they contract of any breaches of health information in their possession, or that they become aware of (and that entity must then notify the individual).

The requirements for timeliness, method and content of notification are the same as those for breach notification by HIPAA-covered entities. The standard for breach, however, is different. A breach is defined as the acquisition of "unsecured PHR identifiable health information of an individual in a personal health record" without the individual's authorization. Entities are not required to notify if the information was protected by a technology specified by the HHS Secretary (following the standards adopted for breaches by HIPAA-covered entities).

Entities required to notify individuals must also notify the Federal Trade Commission (FTC), which is tasked with enforcing these requirements. (The FTC must notify HHS of breaches.) Failure to provide the required notification constitutes an unfair and deceptive act or practice in violation of the Federal Trade Commission Act.

The breach notification requirements are classified as "temporary" in the legislation, but they do not sunset until Congress enacts new legislation establishing requirements for breach notification for non-HIPAA covered entities (and the regulations implementing any new legislation have been promulgated).

> **Regulations/Standards:** The FTC is required to promulgate interim final regulations by August 18, 2009.
> **Effective Date:** Apply to breaches that are discovered on or after 30 days after publication of interim final regulations (September 18, 2009).

Study by HHS (with FTC) on Privacy and Security Protections for Non-Covered Entity PHRs and Related Entities

Under section 13424(b) of ARRA, HHS, in consultation with the FTC, is required to conduct a study and submit a report to Congress on privacy and security requirements for entities that are not covered entities or business associates under HIPAA, including:

- Requirements relating to breach notification for those entities that will be subject to the FTC's new breach notification authority;
- A determination of which federal government agency is best equipped to enforce any recommended privacy and security protections (including breach notification); and
- A timeframe for implementing regulations based on such findings.

Congress stopped short of directing either or both agencies to proceed to rulemaking to impose the recommended protections. The study and report must be completed **within one year of enactment (by February 18, 2010).**

Miscellaneous: Administration/Studies/Reports/Educational Initiatives

Administration Changes

Title XIII subtitle A of ARRA statutorily established the Office of the National Coordinator (ONC) for Health IT and gives it clearer direction and authority. ARRA also establishes a new advisory committee infrastructure, with a new HIT Policy Committee and a new HIT Standards Committee; both are governed by the Federal Advisory Committee Act (FACA). In particular, Section 3002 in the legislation directs the HIT Policy Committee to develop a policy framework for the adoption and implementation of a nationwide health information technology infrastructure and to establish priorities for the development and implementation of health IT standards. Relevant to privacy, the HIT Policy Committee is required to make recommendations with respect to technologies that protect privacy and promote security in an electronic health record, including those that allow for the segregation of sensitive health information and the use of limited data sets. The Policy Committee's recommendations also must prioritize the development of standards to facilitate the new accounting for disclosures requirements for HIPAA-covered entities and business associates.

The legislation also creates a position of Chief Privacy Officer within ONC, who will advise the National Coordinator on privacy, security and data stewardship of

electronic health information (Section 3001(e)). This CPO is not specifically charged with oversight of HIPAA. The legislation also directs the HHS Secretary to designate an individual in each HHS regional office to offer guidance and education to entities and individuals on their rights and responsibilities related to federal privacy and security requirements for protected health information (Section 13403).

Studies/Reports

GAO, HHS and the FTC are directed to conduct a number of studies and issue reports under ARRA (Section 13424 for most).

GAO Reports

- Methodology for providing individuals with a percentage of civil monetary penalties (see above – **due August 18, 2010**)
- Report on best practices related to disclosure among health care providers of protected health information for purposes of treatment of an individual, which must include an examination of the use of electronic informed consent for disclosing protected health information for treatment, payment and health care operations. **Due February 18, 2010.**
- Report on impact of any of the provisions of ARRA on health insurance premiums, overall health care costs, adoption of electronic health records, and reduction in medical errors and other quality improvements. **Due February 18, 2014.**

HHS/FTC Studies

- Annual report to Congress on enforcement of HIPAA. **First report due February 18, 2010 and annually thereafter.**
- Study and report (with FTC) on application of privacy and security requirements to non-HIPAA covered entities (as described above). **Due February 18, 2010.**
- Study on implementation of the HIPAA de-identification provisions. **Due February 18, 2010.**
- Study of HIPAA definition of psychotherapy notes with respect to whether the definition should include test data and materials used by mental health professionals for evaluative purposes. The Secretary may issue regulations to revise the definition based on the study. **No deadline for completion of the study.**

Educational Initiatives

Section 13403 of ARRA directs HHS to develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of protected health information. This initiative must include education of individuals

about potential uses of their protected health information, and their rights with respect to those uses, as well as the "effects" of such uses. The programs have to be offered in a variety of languages and must present information in a way that is clear and understandable. **Must be completed within 12 months (by February 18, 2010).**

For further information, contact: Deven McGraw, Director of the Health Privacy Project at CDT, 202-637-9800 x 119.

Appendix A – Calendar of Due Dates/Effective Dates

Upon enactment (February 17, 2009):

- Application of new tiered civil monetary penalties (for offense occurring post-enactment)
- State AG Enforcement (same)

Within 60 days of enactment (April 20, 2009):

- HHS Secretary must set forth list of technologies and methodologies that render information "unusable, unreadable or indecipherable" (relevant for breach notification provisions)

Within 180 days of enactment (August 18, 2010):

- HHS and FTC must each promulgate interim final regulations on breach notification (apply to breaches discovered on or after the interim final regulations have been published)

By 12/31/2009:

- HHS must adopt (through rulemaking) the initial prioritized set of standards (which should include the accounting for disclosures new technical standard – regs to implement that standard are due 6 months after the technical standard has been adopted)

Due within one year post enactment (February 18, 2010):

- HHS (& FTC) study on privacy and security requirements for PHR vendors and applications
- GAO study on best practices for disclosures for treatment (and use of electronic informed consent)
- First annual report on HIPAA enforcement
- First annual guidance on the most effective and appropriate technical safeguards for health information
- HHS study on de-identification
- HHS implements health information privacy educational initiative

Effective one year post enactment (February 18, 2010):

- Application of rules to, and accountability for, business associates
- Clarification of which entities are required to be business associates (although arguably already accomplished for most RHIOs & HIEs through HIPAA guidance issued by HHS in December 2008)
- Right to restrict disclosures to health plans
- Deeming of limited data set as satisfying minimum necessary standard
- Right of electronic access/electronic copy
- Clarification of marketing provisions
- Opt-out for fundraising communications (although current HIPAA Privacy Rule provisions remain in effect)
- Clarification of ability to impose criminal penalties against individuals

- Civil monetary penalties and settlements flowing to OCR for enforcement
- Requirement for Secretary to periodically audit entities covered by HIPAA

Within 18 months of enactment (August 18, 2010):

- Secretary's guidance on minimum necessary
- Regulations re: sale of data prohibition (effective 6 months post promulgation)
- GAO report on methodology for providing individuals with a percentage of HIPAA penalties
- Regulations on imposition of civil monetary penalties in cases of willful neglect (and with respect to when the Secretary can civilly pursue violations of HIPAA that qualify as criminal)

January 1, 2011:

- Initial deadline for complying with new accounting for disclosure rules for entities implementing electronic record systems after 1/1/09

24 months post enactment (February 18, 2011):

- Clarification of ability to pursue civil penalties when criminal penalties are not pursued (applies to violations discovered on or after)
- Requirement to impose civil monetary penalties in cases of willful neglect (same)

Three years post enactment (February 18, 2012):

- Regulations for methodology for providing individuals with a percentage of HIPAA penalties

By 2013:

- Extended deadline for newer systems to comply with new accounting for disclosure rules

January 1, 2014:

- Initial deadline for older systems to comply with new accounting for disclosure rules

Five years post enactment (February 18, 2014):

- GAO study on impact of ARRA

By 2016:

- Extended deadline for older systems to comply with new accounting for disclosure rules

Appendix B: Civil Monetary Penalty Chart

Type of Offense	Minimum	Maximum
Person did not know (and by exercising reasonable diligence would have known) that the person violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations[7]	$50,000 per violation, with an annual maximum of $1.5 million
Violation due to reasonable cause and not willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

[7] Former statutory maximum (changes in the table went into effect on the date of enactment); also maximum that can be imposed by State Attorneys General regardless of the type of violation.