ARRA Accounting of Disclosures Requirements

Aligning Goals with Emerging Regulations

Lead Authors:
Deven McGraw, Director of the Health Privacy Project, Center for Democracy and Technology and Co-Chair, eHI Privacy Work Group; Gerry Hinkley, Co-Chair, Health Care Industry Team, Pillsbury Winthrop Shaw Pittman and Co-Chair, eHI Privacy Work Group

Supporting Authors:
Brian Wagner, Senior Director of Policy and Public Affairs, eHealth Initiative; eHealth Initiative Privacy Work Group Members

Overview

This paper summarizes the origins of the accounting of disclosure requirements under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the subsequent modifications introduced by the Health Information Technology for Economic and Clinical Health (HITECH) provisions of the American Recovery and Reinvestment Act of 2009 (ARRA) in response to the increasing digitization of patients' protected health information (PHI).[1] In addition, the paper sets out some of the key issues and unanswered questions prompted by the ARRA modifications and sets out some potential approaches for resolving them.

Background

In ARRA, Congress made broad changes to the HIPAA Privacy Rule, including an expansion of the scope and application of the accounting of disclosures requirement. Prior to ARRA, covered entities were required to provide upon request an accounting of disclosures of PHI made in the six years prior to the request. However, disclosures made for purposes of treatment, payment, and healthcare operations, as well as a handful of other disclosures, were exempt. Covered entities also were required to provide an accounting of disclosures made by their business associates. Under ARRA, covered entities that use or maintain an electronic health record (EHR) may no longer rely on the exemption for treatment, payment, and operations and they must account for these (TPO) disclosures over the previous three years. Covered entities may continue to account for disclosures made by business associates or direct patients to request an accounting directly from the business associates. The modifications to the accounting requirements go into effect on January 1, 2011 (or the date of EHR adoption if later) for providers who acquire an EHR after January 1, 2009, and on January 1, 2014 for providers who acquired an EHR before January 1, 2009. The Secretary has the option to postpone either date by up to two years (to 2013 and 2016) if necessary.

Legislative Intent of ARRA Accounting of Disclosures Requirement

The underlying goal of the accounting of disclosures requirement is to increase transparency about the number and nature of disclosures of an individual's PHI. Transparency is a consistent element of fair information practices; in this circumstance, the accounting also

[1] The text of the current accounting provisions and the revisions made by ARRA can be found in the Appendix to this document.

gives patients, if they choose to do so, an expanded ability to monitor disclosures of their information, including in cases of noncompliance with the HIPAA Privacy Rule. The original requirement in the HIPAA Privacy Rule sought to accomplish this goal while also minimizing the burden on industry of producing an accounting. Consequently, only those disclosures that were arguably not "routine" were required to be included, although the accounting needed to cover a six-year period.

As patients' PHI is increasingly moving from paper to digital forms through the adoption of EHRs by HIPAA covered entities and their business associates, the patient privacy landscape is rapidly evolving to adapt to the changing needs of a digital environment. While digitized patient data may in some ways be easier to protect from inappropriate access than data in paper form, the ease of digital data transmission and the sheer volume of data that can be collected in a digital universe creates new challenges for patient privacy protection. In response to this evolving environment, Congress modified the accounting of disclosures requirements to address the increased risk to privacy created by the new digital environment, while also trying to take advantage of technology's theoretical ability—still developing in practice—to automatically generate and disseminate information about accesses and disclosures of electronic records. The challenge now faced by regulators is to implement the new requirements in a way that increases transparency without being excessively burdensome to industry.

Key Issues and Questions

The changes to accounting of disclosures requirements will have a significant impact on covered entities and business associates that use or maintain EHRs and will provide transparency for individuals who proactively seek out data about disclosures of their PHI. Of most significance for covered entities is the elimination of the exemption for disclosures for treatment, payment, and operations, which will greatly increase the number of disclosures that will likely be required to be included in an accounting, notwithstanding the reduction of the time period applicable to accounting for disclosures of TPO from six to three years. Business associates also will be required to account for a greater number of disclosures and will for the first time be required to provide an accounting directly to individuals in some cases.

The language of ARRA requires the adoption of a standard for EHRs to ensure that they have the technical capability to generate a more comprehensive accounting of disclosures, as well as the promulgation of regulations to implement the changes. Among the many challenges faced by HHS in implementing the new provisions include:

- Defining the scope of the new accounting requirements, including the scope of disclosures to be included and how much information is to be provided about each disclosure;
- Clarifying the definition of electronic health record;
- Considering which business associates are covered and how they will comply;
- Managing the short timeline for developing the technical standard, which in the statute precedes the development of regulations that typically serve as the vehicle for resolving substantive policy issues that need to be incorporated into the technical standard;

- Implementing the effective date for the new provisions, which may be too soon to allow covered entities and business associates to achieve compliance; and,

- Dealing with compliance issues faced by smaller providers.

Overall, HHS needs to consider how to implement the new provisions in a way that minimizes the burden to the healthcare industry while also ensuring that patients are provided with information that they understand and is meaningful to them.[2] Effectively addressing these challenges will require input from multiple stakeholders in order to achieve workable technical and policy solutions. Set forth below is a more detailed discussion of these issues as well as some suggestions from the eHI Privacy Work Group about ways to resolve them.

1. Scope of New Accounting Requirement

The current HIPAA accounting of disclosures requirement is found entirely in the Privacy Rule. In ARRA Congress made a few statutory modifications to the existing regulation, but HHS has full discretion to change all of the provisions in the regulation — as long as the changes are not inconsistent with ARRA. For example, while the statute eliminates the treatment, payment, and operations exemption from the current accounting rules for providers using EHRs, HHS still has fairly broad discretion to redefine the scope of what needs to be included in an accounting. For example, HHS may want to consider:

- What disclosures (as the term "disclosure" is currently defined in the HIPAA regulations) will be required to be included in an accounting;

- What information will need to be included in the accounting, and at what level of detail (for example, information recipient, date of disclosure, purpose); and

- How information on disclosures can be conveyed in a way that is meaningful for individuals.

In making these determinations, HHS will need to look at the technical ability of EHRs today and potentially in the future to generate a more complete accounting, as well as the utility of the information to patients. In resolving these issues, HHS could consider (and each of the options below would need to be further explored for policy and technical implications):

- Requiring accounting of disclosures to be provided in stages – individuals would first be provided upon request with a description of where information is disclosed from patient EHRs and for what purposes; those individuals seeking more detailed information about their own record would have to make a second (and potentially more specific) request.

- Deeming an electronic audit trail of all access to the EHR to satisfy the accounting of disclosures requirement. Although auditing all record access goes beyond an accounting of just disclosures, audit trail standards already exist, CCHIT standards for inpatient and ambulatory EHRs established during the Bush Administration

[2] Understanding what patients would ideally want from an accounting is also a challenge; providers report that patients rarely request an accounting of disclosures under current rules. However, whether this low uptake by patients is due to lack of interest, lack of knowledge that such a right exists, or a sense that the accounting today does not include sufficient information to be worth obtaining, is unclear.

already require this for certification, and the Interim Final Rule on certification criteria released by the Obama Administration in December 2009 also requires an audit log.[3] However, such audit logs or trails are often difficult for patients to comprehend; to make this meaningful to patients may mean requiring covered entities to devote time to explain them to patients who have questions, or providing incentives for the development of technical capabilities to translate the results of an audit trail into a simpler format.

- If it is not technologically feasible for EHRs today to generate an accounting that automatically includes some sense of the purpose for each disclosure, consider phasing in such a requirement over time, to allow the technology to develop this capability. Another approach would be to provide incentives or otherwise encourage vendors to release new EHRs (or upgrades) that allow users to select from a list of common disclosure purposes or that otherwise allow for the disclosure purpose to be logged without the need to manually input text.

- If the requirements for accounting are comprehensive (i.e., all or most disclosures; some indication of purpose), HHS should consider approaching Congress about reducing the statutory requirement for the accounting period from three years to a time period that is more feasible (particularly if both consumer and industry stakeholder groups are in agreement on the need for a change).

2. Definition of Electronic Health Record

The revisions to the HIPAA accounting rule apply to those covered entities using EHRs. EHR is defined in the statute 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."[4] A number of stakeholders have expressed concern that the definition is broad enough to encompass all business records kept electronically by a covered entity or business associate. Others raise concerns that EHRs are often not a single software program but instead a collection or system software programs running on disparate hardware that together make up an EHR , potentially introducing new challenges to defining where "disclosures" need to be tracked for accounting purposes. Since the purpose of the ARRA revisions to the accounting rule was to increase the scope of disclosures and not necessarily to give individuals access to records that they do not have the right to access today, HHS should consider clarifying the definition so that it is clear that the accounting addresses only those portions of the record that individuals have the right to access under C.F.R. 164.524.

3. Requirements for Business Associates

Under ARRA, business associates are required to comply with the privacy provisions that apply to covered entities;[5] thus, the new accounting requirements are made applicable to business associates. In addition, ARRA also includes express provisions requiring business associates to directly comply with requests for accounting in some circumstances. The

[3] According to the criteria, the date, time, patient identification (name or number), and user identification (name or number) must be recorded when electronic health information is created, modified, deleted, or printed. An indication of which action(s) occurred must also be recorded (e.g., modification).
[4] ARRA Section 13001, Subtitle A, Part 1, Subtitle D, Section 13400 (5).
[5] ARRA Section 13404(a).

covered entities with which they contract determine whether individuals obtain an accounting of business associate disclosures from the covered entity (which would require the business associate to provide them to the covered entity), or directly from the business associate. Determining how this will take place will need to be covered in the business associate agreement, and some stakeholders would prefer greater regulatory guidance to reduce uncertainty.

HHS should also consider whether, as a result of the new accounting rules, some business associates will now be required to store data for longer that they otherwise would. HHS should balance the benefit of accounting of disclosures against the risk of having to store data for longer than would otherwise be the case.

Although ARRA makes the new accounting provisions applicable to business associates, it is less clear whether this is limited only to those business associates using EHRs. Only those covered entities using EHRs are required to comply with the new provisions; and one could argue that only business associates of covered entities using EHRs are required to comply with the new requirements. But does the EHR limitation also apply to business associates? Limiting business associate coverage to only those using EHRs could greatly limit the scope of coverage of the new provision, as it is unclear, given the definition of EHR, how many business associates use EHRs. At a minimum, business associates actually using EHRs should be covered (which should extend to those business associates using EHRs that also qualify as covered entities [but often serve in business associate roles], as they will already need to be in compliance in their capacity as covered entities). As HHS has full discretion in determining the scope of the rule, the Department should consider making the new provisions applicable to business associates who keep records electronically but who may not technically be using an "EHR" as defined in ARRA.

HHS will also need to determine how entities like Health Information Exchanges and Regional Health Information Organizations (collectively, HIEs) will comply with the new provisions, as ARRA requires them to be business associates.[6] ARRA makes it clear that the covered entity decides whether to account for disclosures from a business associate like an HIE or to tell the patient to get the accounting directly from the HIE. However, depending on the architecture of the data exchange, accounting for "disclosures" may be difficult to track. For example, a federated exchange that merely facilitates the exchange of information by partner or "node" health care organizations may not be able to easily account for disclosures of an individual patient's information (although the partner organizations should be fully accountable for accounting for disclosures through the network). However, HIEs that operate database or even hybrid federated/database models may face no more challenges to accounting for disclosures than a large provider using an EHR.

4. Timeline for (and feasibility of) Technical Standard and Implementing Regulations

ARRA requires the Office of the National Coordinator for Health IT (ONC) to adopt a technical standard to be incorporated into electronic health record (EHR) technology by December 31, 2009, to ensure that EHRs are able to generate and issue an accounting of disclosures. Once the standards are adopted, ARRA gives HHS (presumably the Office of Civil Rights (OCR)) up to six months to promulgate regulations on the information that needs to be collected on each relevant disclosure. The regulations must take into account

[6] ARRA Section 13408.

the needs of patients, as well as the burden placed on covered entities and business associates. ONC adopted basic certification criteria to provide a technical foundation for the new accounting provisions in an Interim Final Rule released in prepublication version on December 30, 2009.[7]

As noted above, proponents of the ARRA modifications to the accounting of disclosures provisions envisioned that EHR technology would be able to "automatically" generate a record of disclosures. For this to occur, the technical standard should address the level of technical functionality needed to fully comply with the new requirements. But decisions about the scope of the disclosure requirement (i.e., what information needs to be included in the accounting) are typically be resolved in regulations, which HHS is not required to promulgate until six months *after* the standard has been issued. Similarly, OCR, in developing the specifics of the regulations, will need to consider what is technologically feasible.

ONC has adopted a standard requiring certified EHRs to be able to record the date, time, patient identification (name or number), user identification (name or number), and a description of treatment, payment and operations (TPO) disclosures. ONC intends for to provide the technical foundation for later rulemaking by the Secretary that will flesh out more of the details of how entities will need to comply with the new accounting provisions. ONC acknowledges that there remain significant technical challenges that will need to be addressed. For example, what needs to be included in each disclosure lacks specificity; is it possible for EHR systems to distinguish between a "use" and a "disclosure" as those terms are defined by HIPAA; and how much electronic storage will be needed to record three years of information on TPO disclosures.[8] In addition, it's not clear whether the initial criteria can be accomplished by existing EHR systems, or if the criteria lay a sufficient technical foundation for regulations to be developed by OCR. The Interim Final Rule is subject to a 60 day comment period and could be subject to modification.

5. Effective Date

The new accounting requirements go into effect in 2011 for providers "acquiring" EHRs after January 1, 2009; the Secretary can extend this deadline by up to two years if necessary. For those providers acquiring systems before January 1, 2009, the technology is not expected to incorporate the new standard and is not required to meet the new requirements until 2013. Similarly, providers acquiring a system between the enactment of ARRA and the promulgation of the technical standard and regulations will have no idea if they will be able to meet the compliance requirements by the deadline. In addition, it is unclear how much lead time vendors will need to be able to incorporate any new technical standard into their EHR technology. In addition, how is the term "acquire" to be defined – is it triggered by the signing of a purchase or license agreement, or deployment or implementation? Also, how will business associates manage compliance when the covered entities with which they contract may be subject to different (likely the earliest possible) effective date? The Secretary should take all of this into account in considering whether or not an extension of the compliance deadline is appropriate. (ONC's Interim Final Rule on certification criteria expressly notes that "the Secretary will address the compliance date for accounting for [TPO] disclosures in a later rulemaking."[9]

---

[7] http://www.federalregister.gov/OFRUpload/OFRData/2009-31216_PI.pdf

[8] http://www.federalregister.gov/OFRUpload/OFRData/2009-31216_PI.pdf, see pages 91-92.

[9] Id. at 92.

6. Burden on Small Providers

While in the past covered entities using EHRs have typically been viewed as large hospital systems, financial incentives in ARRA were designed to stimulate the adoption of EHRs in the ambulatory setting, including in practices as small as a single physician office. In addition, the technical capabilities of EHRs used in the ambulatory versus inpatient setting vary significantly. In fleshing out the scope of the new accounting requirements, HHS should consider whether there should be some flexibility in the requirements to avoid imposing undue financial and administrative burdens on smaller providers who typically do not have adequate staff or resources.

Final Thoughts

The ARRA accounting of disclosure provisions will be a challenge to implement, but the regulatory process does offer important opportunities for stakeholders to ensure they are implemented in a way that accomplishes the stated goals achieved by giving patients the right to an accounting without placing an undue burden on covered entities and business associates. Given the potential impact of the new provisions and the short timeframe in which the issues must be resolved, quick and thoughtful inputs from both industry and consumer stakeholders are critical.

Appendix

§ 164.528 Accounting of disclosures of protected health information.

(a) Standard: right

(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in § 164.502;

(ii) To individuals of protected health information about them as provided in § 164.502;

(iii) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;

(iv) For national security or intelligence purposes as provided in § 164.512(k)(2);

(v) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5); or

(vi) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) Implementation specifications: content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) The accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:

(A) A copy of the individual's written authorization pursuant to § 164.508; or

(B) A copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, or pursuant to a single authorization under § 164.508, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(c) Implementation specifications: provision of the accounting.

(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) Implementation specification: documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

ARRA Section 13405(c)

(c) ACCOUNTING OF CERTAIN PROTECTED HEALTH INFORMATION DISCLOSURES REQUIRED IF COVERED ENTITY USES ELECTRONIC HEALTH RECORD.—
''(1) IN GENERAL.—In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information—
''(A) the exception under paragraph (a)(1)(i) of suchsection shall not apply to disclosures through an electronic health record made by such entity of such information; and
''(B) an individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting
is requested.
''(2) REGULATIONS.—The Secretary shall promulgate regulations on what information shall be collected about each disclosure referred to in paragraph (1), not later than 6 months after the date on which the Secretary adopts standards on accounting for disclosure described in the section 3002(b)(2)(B)(iv) of the Public Health Service Act, as added by section 13101. Such regulations shall only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures.
''(3) PROCESS.—In response to an request from an individual for an accounting, a covered entity shall elect to provide either an—
''(A) accounting, as specified under paragraph (1), for disclosures of protected health information that are made by such covered entity and by a business associate acting on behalf of the covered entity; or
''(B) accounting, as specified under paragraph (1), for disclosures that are made by such covered entity and provide a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address). A business associate included on a list under subparagraph (B) shall provide an accounting of disclosures (as required under paragraph (1) for a covered entity) made by the business associate upon a request made by an individual directly to the business associate for such an accounting.
''(4) EFFECTIVE DATE.—
''(A) CURRENT USERS OF ELECTRONIC RECORDS.—In the case of a covered entity insofar as it acquired an electronic health record as of January 1, 2009, paragraph (1) shall apply to disclosures, with respect to protected health information, made by the covered entity from such a record on and after January 1, 2014.
''(B) OTHERS.—In the case of a covered entity insofar as it acquires an electronic health record after January 1, 2009, paragraph (1) shall apply to disclosures, with respect to

protected health information, made by the covered entity from such record on and after the later of the following:
''(i) January 1, 2011; or
''(ii) the date that it acquires an electronic health record.
''(C) LATER DATE.—The Secretary may set an effective date that is later that the date specified under subparagraph (A) or (B) if the Secretary determines that such later date is necessary, but in no case may the date specified under—
''(i) subparagraph (A) be later than 2016; or
''(ii) subparagraph (B) be later than 2013.''

Technical Standard (Interim final rule released 12/30/2009)

45 CFR Part 170

170.210 The Secretary adopts the following standards to protect electronic health information
created, maintained, and exchanged:

(e) Record treatment, payment, and health care operations disclosures. The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.

170.302 The Secretary adopts the following general certification criteria for Complete EHRs or
EHR Modules. Complete EHRs or EHR Modules must include the capability to perform the following functions electronically and in accordance with all applicable standards and implementation specifications adopted in this part:

(v) Accounting of disclosures. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in §170.210(e).