

HIPAA Privacy Rule Accounting for Disclosures under the Health Information Technology for Economic and Clinical Health Act

Summary of Proposed Rule

Introduction

On May 31, 2011, the Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) published a proposed rule that OCR claims would implement the statutory requirement under the Health Information Technology for Economic and Clinical Health Act (HITECH) to require covered entities and business associates to account for disclosures of protected health information to carry out treatment, payment, and health care operations if such disclosures are through an electronic health record (EHR). Under its more general authority under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department also proposes changes to the existing accounting requirements “to improve their workability and effectiveness.”

OCR also proposes to “expand the accounting provision to provide individuals the right to receive an access report indicating who has accessed electronic protected health information in a designated record set” [emphasis added].

Comments on the proposed rule are due by August 1, 2011.

OCR contemplates publishing the final rule in late 2011.

Background

The Privacy Rule at 45 CFR 164.548 requires covered entities to make available to an individual upon request an accounting of certain disclosures of the individual’s protected health information made during the six years prior to the request. A disclosure is defined at § 160.103 as “the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information” [emphasis added]. Section 164.528(a)(1) provides that an accounting must include all disclosures of protected health information except certain specified disclosures (for example, those to carry out treatment, payment and health care operations, for national security or intelligence purposes, and to correctional institutions or law enforcement officials).

The current accounting provision applies to disclosures of paper and electronic protected health information. In addition, an accounting provided by a covered entity must include disclosures to and by its business associates.

Section 13405(c) of HITECH provides that the exemption for disclosures to carry out treatment, payment and health care operations (mentioned above) no longer applies to disclosures through an EHR, and HITECH defines an EHR 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.” Under § 13405(c), an individual has a right to receive an accounting of such disclosures made during the three years prior to the request. Further, with respect to disclosures by business associates through an EHR to carry out treatment, payment, and health care operations on behalf of the covered entity, the statute requires the covered entity to provide either an accounting of the business associates’ disclosures, or a list and contact information of all business associates (enabling the individual to contact each business associate for an accounting of the business associate’s disclosures).

In an interim final rule published on January 13, 2010, the Office of the National Coordinator for Health Information Technology (ONC) adopted a standard and certification criterion to account for disclosures. The standard and certification criterion provide that certified EHR technology have the capability to record the date, time, patient identification, user identification, and a description of the disclosure, for disclosures made for treatment, payment, and health care operations. However, a final rule published on July 28, 2010 made this certification criterion optional, meaning that EHR technology is not required to have this capability as a condition of certification for meaningful use Stage 1 under the Medicare and Medicaid EHR incentive payment programs.

HITECH provides that the effective date of the accounting requirement for HIPAA covered entities that have acquired an EHR after January 1, 2009 is January 1, 2011, or the date that it acquires an EHR, whichever is later. For covered entities that acquired EHRs prior to January 1, 2009, the effective date is January 1, 2014. However, the statute authorizes the Secretary to extend both of these compliance deadlines to no later than 2013 and 2016, respectively.

OCR also notes that on May 3, 2010, HHS published a request for information, which posed nine questions seeking further information on individuals’ interests in learning of disclosures, the burdens on covered entities in accounting for disclosures, and the capabilities of current technology. HHS received about 170 comments in response to this request for information and briefly summarizes them in the proposed rule.

Accounting of Disclosures of Protected Health Information

The intent of the accounting of disclosures is to provide detailed information for certain disclosures that are most likely to impact the individual. The right to an accounting of disclosures would encompass disclosures of both hard copy and electronic protected health information that is maintained in a designated record set. An accounting of disclosure would need to include the applicable disclosures of a covered entity’s business associates, although OCR believes that some business associates will not be affected by the proposed new requirements because they do not have designated record set information.

OCR proposes a number of changes to the right of an individual to receive an accounting of disclosures by a covered entity or business associate. First, OCR proposes to limit the accounting provision to protected health information about the individual in a designated record set, and notes that designated record sets include “the medical and health care payment records maintained by or for a covered entity, and other records used by or for the covered entity to make decisions about individuals.” OCR gives as examples of protected health information that may fall outside the designated record set a hospital’s peer review files (if they are only used to improve patient care at the hospital, not to make decisions about individuals) and transcripts of customer calls that are used only for purposes of customer service review.

Second, OCR proposes to require that a covered entity must include accounting information for all disclosures by its business associates within a designated record set, a change from current requirements that apply without regard to whether the information is within a designated record set.

Third, since HITECH states that an individual has a right to receive an accounting of treatment, payment, and health care operations disclosures through an EHR for the 3-year period prior to the request, OCR proposes to change the current accounting period from 6 years to 3 years to maintain a consistent accounting period for all types of disclosures.

Fourth, the proposed rule explicitly lists the types of disclosures that would be subject to the accounting requirement (rather than the current practice of listing exemptions). These include the following:

- Disclosures not permitted under the HIPAA Privacy Rule unless the individual has received notification of the impermissible disclosure (that is, a breach notice) pursuant to § 164.404;
- For public health activities as provided in § 164.512(b), except disclosures to report child abuse or neglect (in response to concerns about the potential harm a covered entity or members of its workforce may suffer if they have to account to a parent or guardian for its reporting to authorities of suspected child abuse or neglect);
- For judicial and administrative proceedings as provided in § 164.512(e);
- For law enforcement purposes as provided in § 164.512(f);
- To avert a serious threat to health or safety as provided in § 164.512(j);
- For military and veterans activities, the Department of State’s medical suitability determinations, and government programs providing public benefits as provided in § 164.512(K)(1), (4), and (6); and
- For workers’ compensation as provided in § 164.512(l).

Further, except for disclosures for judicial and administrative proceedings, and those for law enforcement purposes, a covered entity need not account for other disclosures listed above if they are required by law. In this regard, OCR carefully distinguishes between disclosures required by law as opposed to those merely authorized (the proposed exemption would not apply to authorized disclosures).

Rather curiously, although the proposed rule does not explicitly say so, the new regulatory construct described above (which lists specific disclosures that must be accounted for) would mean that future accountings of disclosures would not need to include all disclosures for treatment, payment, and health care operations even though made through an electronic health record. In contrast, the proposed, new access reports (discussed in detail below) would need to include information about persons who accessed certain protected health information for treatment, payment, and health care operations purposes.

OCR requests comments on the following issues:

- Whether there are categories of public health disclosures (other than those to report child abuse or neglect) that warrant an exception and whether the complexity of carving out such public health disclosures would lead to too much confusion;
- Whether HHS should exempt from the accounting requirements certain categories of disclosures that are currently subject to the accounting.

OCR adds that it is proposing to exclude disclosures about victims of abuse, neglect, or domestic violence; those for health oversight activities; disclosures for research purposes, including through a protocol listing, which is a simpler accounting method for larger studies; disclosures about decedents to coroners and medical examiners, funeral directors, and for cadaveric organ, eye, or tissue donation purposes; disclosures for protective services for the President and others; and most disclosures that are required by law (including those to HHS to enforce the HIPAA Administrative Simplification Rules).

With reference to research disclosures, OCR solicits comments on the value of the current accounting for research disclosures to individuals who have used or might in the future request such an accounting. OCR also asks covered entities to provide data regarding the number of protocols that would typically be included in a protocol listing, the nature and number of smaller research studies that involve the disclosure by the covered entity of protected health information about less than 50 individuals and for which a specific accounting is currently required, and the burdens on researchers and covered entities to provide the requested accountings of disclosures. In addition, OCR seeks comment on alternative, less burdensome ways that individuals could be provided information about the covered entity's research disclosures, such as the Institute of Medicine's recommendation for a list of all Institutional Review Board/Privacy Board-approved studies.

OCR concludes that accounting for disclosures that are made through electronic health information exchange (for example, when a covered entity or business associate transmits some or all of an EHR to another electronic system, such as another covered entity's EHR, a pharmacy, laboratory, or health plan) "at this time would be overly burdensome when compared to the potential benefit to individuals." However, OCR adds that as electronic health information exchange

expands and standards for such exchange are adopted, it intends to work with ONC to assess whether such standards should include information about the purpose of each exchange transaction.

OCR also proposes that a covered entity must exclude from accountings of disclosures any information that meets the definition of patient safety work product at 42 CFR 3.20.

OCR notes that if a covered entity has been subject to the HIPAA Privacy Rule for less than 3 years, then it would only need account for the period of time during which it was subject to the Rule.

With respect to the content of the accounting of disclosures, OCR proposes that a covered entity or business associate need only provide an approximate date or period of time for each disclosure, if the actual date is not known (at minimum, a month and year or a description of when the disclosure occurred from which an individual can readily determine the month and year of disclosure, such as “within 15 days of discharge”). For multiple disclosures to the same person or entity, the approximate period of time would be sufficient (an exact start date and end date would not be required).

The accounting would also need to include the name of the entity or natural person who received the protected health information and, if known, their address. However, OCR proposes an exception when providing the name of the recipient would itself represent a disclosure of protected health information about another individual (in such cases, for example, the accounting could simply indicate that the disclosure was to “another patient” or “another enrollee” or similar language).

OCR also proposes that the accounting include a brief description of the type of protected health information disclosed (sadly, no further explanation is given of what is meant by “type”). Further, the accounting would need to include a brief description (what OCR later labels as “only a minimum description”) of the purpose of the disclosure, such as “for public health” or “in response to law enforcement request.” OCR proposes to retain regulatory language indicating that a copy of a written request may be substituted for a description of the purpose of the disclosure, and encourages covered entities to provide such a copy when it provides more information than the general “purpose” description in the accounting.

OCR proposes to require that covered entities provide individuals the option of limiting the accounting to a particular time period, type of disclosure, or recipient (such as disclosures by a particular business associate).

With respect to providing a requested accounting of disclosures, OCR proposes to: (1) decrease the permissible response time from 60 days to 30 days (while

retaining the availability of a 30-day extension); (2) require covered entities to provide the accounting in the form (paper or electronic) and format (e.g., compatibility with a specific software application, such as a PDF file or a format compatible with a particular word processor) requested by the individual if readily producible; and (3) clarify that the covered entity may require the individual to submit an accounting request in writing. If the requested form and format is not readily producible, a covered entity may provide a hard copy or the parties may try to determine if another form and format is acceptable. OCR emphasizes that it is not proposing to require that the accounting be provided in electronic form, unless it is readily producible in such form. OCR also adds that a covered entity is not responsible or liable for the information once it is in the individual's possession (for example, if the requesting individual does not want an electronic file to be encrypted or password protected). OCR encourages covered entities to create forms for individuals to request an accounting that inform individuals of the information that will be included and allow individuals to narrow the request based on their interests.

OCR reminds readers that a covered entity may not charge for the first request for an accounting in a 12-month period but may charge a reasonable and cost-based fee for providing subsequent requests in the same 12-month period. The proposed rule would require covered entities to inform the individual at the time of the first accounting request that all subsequent requests in the 12-month period may be subject to a fee, and would require them to inform individuals making such subsequent requests of the fee (at the time of a subsequent request) and provide such individuals with an opportunity to withdraw or modify (for example, narrow) their request in order to avoid or reduce the fee.

OCR proposes to retain the requirement for covered entities to delay the provision of an accounting for disclosures based on an ongoing law enforcement investigation (while clarifying that if law enforcement requests a delay, a covered entity must still account for all other disclosures and then supplement the accounting with information about the law enforcement disclosures upon expiration of the requested law enforcement delay).

OCR proposes two changes to existing documentation requirements related to accounting for disclosures. First, a covered entity must maintain documentation necessary to generate an accounting of disclosures for 3 years (rather than the current 6 years); OCR nevertheless observes that covered entities and business associates may choose to retain the information longer based on other legal requirements or internal policies. Second, OCR clarifies that a covered entity must retain a copy of the accounting provided to an individual (not the original). This copy must be retained for 6 years from the date the accounting was provided. Further, a covered entity must retain documentation of the designation of who is responsible for handling accounting requests for 6 years from the last date the designation was in effect.

Right to an Access Report

OCR proposes to give individuals a new right to an access report (which would include electronic access by both workforce members and persons outside the covered entity). The intent of the access report is to allow individuals to learn if specific persons have accessed their electronic designated record set information. The right to an access report would only apply to protected health information about an individual that is maintained in an electronic designated record set. It would not distinguish between uses and disclosures.

OCR emphasizes that this right does not extend to access to paper records. OCR notes that an access log (also known as an audit trail or audit log) is the raw data that an electronic system containing protected health information collects each time a user accesses information, while an access report (also known as an audit report) is a document that a system administrator or other appropriate person generates from the access log in a format that is understandable to an individual. OCR expects that data from each pertinent access log will be gathered and aggregated to generate a single access report (including data from business associates' systems, which a covered entity would be required to obtain, although OCR believes that some business associates will not be affected by the proposed new requirements because they do not have designated record set information).

In proposing the new right to an access report, OCR notes that in response to its previous request for information, most covered entity commenters indicated that their system is unable to automatically distinguish between uses and disclosures of information. OCR takes this to mean that the inclusion of all access (rather than only access that represents a disclosure) would be less burdensome on covered entities and business associates than the alternative of configuring systems to distinguish between uses and disclosures of information, and later says it expects that the proposed right to an access report will require minimal, if any, changes to existing information systems. OCR further notes that it has included all electronic protected health information in a designated record set, rather than only EHR information, arguing that this "greatly improves transparency and better facilitates compliance and enforcement, while placing a reasonable burden on covered entities and business associates." OCR further believes that limiting the right to an access report to an EHR "would create too much confusion for covered entities, hinder...enforcement efforts, and lead to confusion for individuals who seek to exercise their privacy rights." OCR also emphasizes that the Security Rule already requires covered entities and business associates to maintain access logs, and argues that they should, therefore, be able to provide this information to individuals in response to requests.

As with accountings of disclosures, OCR proposes that a covered entity shall exclude from access reports any information that meets the definition of patient safety work product at 42 CFR 3.20.

With respect to the content of access reports, OCR proposes to require inclusion of the following: (1) the date of access; (2) the time of access; (3) the name of the natural person, if available, otherwise the name of the entity accessing the electronic designated record set information; (4) a description of what information was accessed, if available (with OCR acknowledging that an access report might include some entries that identify what information was accessed, while other entries might leave this field blank); and (5) a description of the action by the user (for example, “create,” “modify,” “access,” or “delete”), if available (not a description of what use or disclosure was ultimately made with the information accessed or to whom the user provided the information). OCR further notes that it intends covered entities to include the start time for access in the access reports, although they are free to also include the end time when it is available. OCR also recognizes that some access logs may rely on user IDs (rather than names) but it expects covered entities to match each user ID with a first and last name. OCR further recognizes that an electronic designated record set system may exchange data with another electronic system within the organization and, in such cases, OCR would permit the access log to identify such access by the name of the covered entity; OCR requests comment on this issue, particularly the burden of providing identifying information about internal systems and the interests of individuals in learning of such internal exchanges. OCR also notes that an access report (in contrast to an accounting of disclosures) need not include the address of any user or a brief statement of the purpose of the disclosure. Nonetheless, OCR requests comment on its assumption that systems do not record information about the purpose of the access and ultimate recipient of the information within audit logs.

In the proposed rule, OCR says it expects that “only a small minority of individuals” would exercise the proposed, new right to an access report. In a footnote, OCR also notes that to the extent a covered entity has a reasonable belief that providing certain information in an access report to a personal representative of an individual would endanger the individual, it may elect not to provide the information pursuant to § 164.502(g)(5) of the Privacy Rule.

As with accounting for disclosures, OCR proposes to require covered entities to provide individuals with the option to limit the access report to a specific date, time period, or person (and states its expectation that audit systems can readily produce an access report limited in this fashion). OCR further recommends (but does not require) covered entities to offer individuals the option to limit the access report to specific organizations. OCR also proposes that covered entities provide access reports in a format that is understandable to individuals (that is, a format “that is structured in a manner so that it reasonably can be understood by individuals without an external aid”). OCR notes, however, that it does not

propose to require any summary information or additional content, such as information about the role of each person who accesses the individual's protected health information. The proposed rule offers the following example of an "understandable" format (although it sidesteps providing an entry for a description of what information was accessed, which the proposed rule says must be provided "if available"):

<u>Date</u>	<u>Time</u>	<u>Name</u>	<u>Action</u>
10/10/2011	02:30 p.m.	John, Andrew	Viewed

With respect to the provision of access reports, OCR proposes a response deadline of 30 days (as for accountings of disclosures), with a 30-day extension, where necessary, "as long as the covered entity provides the individual with a written statement that includes the reason for the delay and the date by which the covered entity will provide the access report." OCR also proposes to require covered entities to provide access reports in the machine readable or other electronic form and format (for example, compatibility with a specific software application) requested by an individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by a covered entity and an individual. If the individual does not agree to accept the readable electronic format that is readily producible, the covered entity may provide a readable hard copy (if a hard copy is requested, it must be a readable hard copy).

As with the accountings of disclosures, a covered entity may not charge for providing the first access report to an individual in any 12-month period, but may charge a reasonable, cost-based amount for each additional access report requested within the 12-month period (which may include the reasonable costs of including access report information of business associates). Also, covered entities must inform the individual at the time of the first access report request that all subsequent requests in the 12-month period may be subject to a fee, and must inform individuals making such subsequent requests of the fee (at the time of a subsequent request) and provide such individuals with an opportunity to withdraw or modify their request in order to avoid or reduce the fee. OCR further proposes to adopt the same documentation requirements for access reports as for accountings of disclosures (see above).

OCR states that covered entities need not revise their notices of privacy practices to reflect the right to receive an access report until the earliest applicable compliance date (see below). OCR also acknowledges that it has been considering ways to inform individuals of changes to privacy practices without unduly burdening health plans, including allowing plans to notify individuals of revisions (either by providing the revised notice or information about the material change and how to obtain the revised notice) in their next

annual mailing to individuals then covered by the plan, rather than within 60 days of the material change.

Effective and Compliance Dates

OCR proposes to require that covered entities (including small health plans) and business associates comply with the modifications to the accounting of disclosures requirement beginning 180 days after the effective date of the final regulation (240 days after publication). As noted earlier, OCR expects to publish this final rule in late 2011.

OCR notes that § 13405(c)(4)(B) of HITECH provides that a covered entity that acquired an EHR after January 1, 2009 must account for disclosures for treatment, payment, and health care operations beginning January 1, 2011 (or the date that it acquires an EHR after January 1, 2011) but also authorizes the Secretary to extend this date to no later than 2013. Further, section 13405(c)(4)(A) of HITECH provides that a covered entity that acquired an EHR as of January 1, 2009, must account for disclosures for treatment, payment, and health care operations beginning January 1, 2014. The statute also authorizes the Secretary to extend this deadline to no later than 2016. Rather curiously, OCR cites all of this as a prelude to specifying its decisions with respect to compliance dates for access reports; in fact, OCR states that the proposed right to an access report “is based in part on the requirement of section 13405(c) of the HITECH Act to provide individuals with information about disclosures through an EHR for treatment, payment and health care operations” (and also based in part on OCR’s general authority under HIPAA).

Specifically, OCR proposes to require covered entities and business associates to produce an access report upon request beginning January 1, 2013 for any electronic designated record set systems that were acquired after January 1, 2009, and beginning January 1, 2014 for electronic designated record set systems that were acquired on or before January 1, 2009. With regard to the latter compliance date, OCR says it does not believe it is necessary to extend the deadline (to no later than 2016), though it claims to have the authority to do so (as cited above). OCR recognizes that during 2013 a covered entity or business associate may be required to produce an access report that includes access to some electronic designated record set systems (those acquired after January 1, 2009) but not others (those acquired as of January 1, 2009). OCR encourages covered entities and business associates in such circumstances to provide access reports that include all designated record set systems during 2013 even if this is not required.

Regulatory Analyses

OCR estimates new total costs of \$20.2 million for covered entities to issue new notices of privacy practices (to account for the new right to receive access

reports). These are labor costs relating to the one-third of an hour of professional, legal time needed for each organization to modify “one sentence” in its existing notice of privacy practices (\$30 times an estimated 673,324 providers and health plans).

OCR acknowledges that there might be other costs relating to the proposed rule, says it is unable to quantify them at this time, and requests more information on:

- The number of anticipated accounting for disclosures and access reports;
- The additional costs, if any, of offering them in electronic formats; and
- The burden of tracking access to electronic designated record set information; and any other additional changes to existing systems that would be necessary.

To comment on the information collection requirements associated with the proposed rule or to obtain copies of the related supporting statement and any related forms, interested parties should e-mail their comment or request, including their address and phone number, to sherette.funncoleman@hhs.gov, or call the Reports Clearance Office on 202-690-6162.