HIPAA/HITECH Act: Accounting of Disclosures Proposed Rule – New Individual Right to Access Report and Significant Changes to Accounting of Disclosures Proposed

On May 31, 2011, the Office of Civil Rights (OCR) of the Department of Health and Human Services (HHS or “the Secretary”) published a notice of proposed rulemaking to modify the HIPAA Privacy Rule’s standard for accounting of disclosures of protected health information. The purpose of the proposed rule is, in part, to implement the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) requirement for covered entities and business associates to account for disclosures of protected health information (PHI) to carry out treatment, payment and health care operations if the disclosures are through an electronic health record (EHR). OCR also proposed to expand the accounting provision to provide individuals with the right to receive an access report for uses and disclosures of electronic PHI in a designated record set, in accordance with HITECH Act requirements.

Notably, OCR proposes to limit the time period for which covered entities and business associates are required to account for disclosures and provide an access report to three years prior to the date of the request. Exercising its authority under HIPAA and the HITECH Act, OCR proposes that the new right to an access report be applicable not just to PHI held in an EHR, but to all electronic PHI held in a designated record set. This means that all covered entities and business associates, not just those covered health care providers who maintain PHI in an EHR, will be subject to the requirement to provide access reports.

Comments on the proposed rule must be submitted by August 1, 2011. This advisory provides a section-by-section summary of the key changes to the HIPAA Privacy Rule.

The Current Privacy Rule and Accounting for Disclosures

Under the current Privacy Rule, covered entities are required to make available to a requesting individual an accounting of certain disclosures of the individual’s PHI made in the six years prior to the request (45 C.F.R. § 164.528). An accounting must include all disclosures of PHI, except for certain specifically excluded disclosures (including disclosures to carry out treatment, payment and health care operations under 45 C.F.R. § 164.506). The current Privacy Rule accounting of disclosures provision applies to disclosures of paper and electronic PHI, regardless of whether the information is in a designated record set. The Privacy Rule defines “designated record set” as “a group of records maintained by or for a covered entity

that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals."³ An accounting may include disclosures to and from a covered entity’s business associates. Under the terms of business associate agreements, business associates are required to make available information on applicable disclosures in order for a covered entity to provide a proper accounting to the requesting individual.

**Changes to the Current Privacy Rule Required by the HITECH Act**

Section 13405(c) of the HITECH Act provides that the accounting of disclosures exemption for disclosures to carry out treatment, payment and health care operations no longer applies to disclosures through an EHR.⁴ Under this section, an individual has the right to receive an accounting of disclosures made up to three years prior to the request. Additionally, Section 13405(c) requires covered entities to provide individuals with either an accounting of the business associate’s disclosures or a list of all of its business associates with contact information. The Secretary is required to promulgate regulations regarding the type of information to be collected in order to provide an accounting of disclosures.

Pursuant to the HITECH Act, the effective date of the new accounting requirements for covered entities that have acquired an EHR after January 1, 2009, is January 1, 2011, or the date that the covered entity acquires an EHR, whichever is later. For covered entities that acquired an EHR prior to January 1, 2009, the effective date is January 1, 2014. The Secretary is permitted to extend these dates to no later than January 1, 2013, and January 1, 2016, respectively.

**The Proposed Rule**

OCR proposes to revise Privacy Rule § 164.528 “by dividing it into two separate rights for individuals”: an individual’s right to an accounting of disclosures, and an individual’s “right to an access report (which would include electronic access by both workforce members and persons outside the covered entity).” ⁷⁶ Fed. Reg. at 31428-29. OCR proposes these changes to improve the workability and effectiveness of the accounting provision. The new right to an access report stems from the requirements of HITECH Act § 13405(c).

OCR views these two rights as distinct but complementary. The access report would provide an individual with information on who has accessed his/her electronic PHI in a designated record set (i.e., an individual can learn if a specific person accessed his/her electronic designated record set). On the other hand, the right to an accounting would provide an individual with information on disclosures of designated record set information, in either paper or electronic form, to persons outside of the covered entity or its business associate for specific purposes (e.g., an individual can learn if PHI was disclosed for law enforcement or judicial hearing reasons). The goal of each right is to provide individuals with valuable information regarding the uses and disclosures of their PHI.

³ For purposes of the definition of “designated record set,” “record” is defined as “any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.”

⁴ An electronic health record is “an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.” HITECH Act § 13400, 42 U.S.C. § 17921.
With respect to business associates and the proposed new rights, covered entities would be required to include the applicable uses and disclosures of their business associates. Some business associates would not be affected by the proposed rule because they do not maintain designated record set information.

Additionally, OCR proposes to revise the notice of privacy practices requirements (§ 164.520), so that individuals are informed of their right to receive an access report, as well as an accounting of disclosures.

The proposed compliance date for the revised accounting of disclosures requirements is 180 days after the effective date of the final regulation (240 days after publication). The proposed compliance date for the access report requirements is January 1, 2013, for covered entities and business associates with electronic designated record set systems acquired after January 1, 2009, and January 1, 2014, for those with electronic designated record set systems acquired as of January 1, 2009. Covered entities would be required to revise their notice of privacy practices by the earliest applicable compliance date for the access report requirements. Under the current Privacy Rule, within 60 days of that date, covered health plans would be required to provide notice to individuals of the change in the notice of privacy practices, although OCR is considering changes to this requirement.

**Accounting of Disclosures – Section 164.528(a)**

In Section 164.528(a), OCR proposes the following changes:

- **Modify the scope of information subject to the accounting requirement to information about an individual in a designated record set.**

OCR proposes to limit the scope of the accounting provision to only the PHI in a designated record set. This proposed change would align the individual’s right to receive an accounting of disclosures with the rights an individual has to access and amend PHI, which are both limited to PHI in a designated record set. Thus, a covered entity would only be required to account for disclosure of PHI made from the record sets used by a covered entity to make decisions concerning the individual, which OCR believes represents the PHI that is of the most interest to the individual.

- **Explicitly include business associates in the language of the rule.**

The proposed rule includes a direct reference to business associates so that covered entities include accounting information for all appropriate disclosures, including those by its business associates that create, receive, maintain or transmit designated record set information. Additionally, the proposed rule limits the accounting information to be reported by business associates to information held by the business associate within a designated record set.

- **Change the accounting period from six years to three years.**

OCR proposes to change the accounting period from six to three years. The current Privacy Rule requires covered entities and business associates to account for disclosures for a six-year period prior to the request. The HITECH Act provides an individual with the right to receive an accounting of treatment, payment and health care operations disclosures through an EHR for a three-year period prior to the request. In an effort to maintain consistency, OCR proposes to align the accounting periods for all accountings to a three-year period. OCR believes that individuals requesting an accounting are interested in the most recent disclosures.
of their PHI. Additionally, OCR believes it is a significant burden on covered entities and business associates to maintain information for a six-year period in order to provide an accounting of disclosures.\textsuperscript{5}

- **List the types of disclosures that are subject to the accounting requirement (rather than listing the types of disclosures that are exempt from the accounting as is currently done in the Privacy Rule).**

The current Privacy Rule provides that an individual has a right to an accounting of disclosures except for a list of specifically exempted disclosures. Under the proposed rule, the types of disclosures that are subject to the accounting requirement would be listed. OCR proposes to make this change because it believes that, under the current Privacy Rule, it may be difficult for covered entities to determine the types of disclosures that are subject to the accounting requirement.

Under the proposed rule, covered entities will continue to account for impermissible disclosures, including those that do not rise to the level of a breach under the Breach Notification Rule.\textsuperscript{6} OCR has proposed, however, to exempt from accounting such disclosures for which a breach notification has been provided to the individual. These disclosures are exempt because the covered entity has already made the individual aware of the impermissible disclosure.

OCR proposes to continue to include, in an individual’s accounting, disclosures for (1) public health activities (except disclosures involving child abuse or neglect reports); (2) judicial and administrative proceedings; (3) law enforcement activities; (4) to avert a serious threat to health or safety; (5) military and veterans activities; (6) Department of State’s medical suitability determinations; (7) government programs providing public benefits; and (8) workers’ compensation. Public health disclosures that are also required by law would not be subject to the proposed accounting requirement. OCR proposes to exempt from the accounting requirement reports of child abuse and neglect because entities have raised concerns about the potential harm that may result to the covered entity (or individual workforce members) from providing to a parent or guardian an accounting that discloses reports to public health or government authorities of suspected abuse or neglect. Apart from this proposed exemption, OCR proposes to maintain the requirement for accounting with respect to these disclosures because it believes that individuals would have significant interest in knowing about such disclosures because they may impact an individual’s legal, employment or benefits interests.

For purposes of an accounting of disclosures, OCR would continue to exclude the disclosures currently listed in the Privacy Rule as exempt from accounting.\textsuperscript{7} Disclosures to carry out treatment, payment and health care operations would continue to be exempt for paper records. Individuals would be able to receive information by means of an access report for all access to electronic PHI in a designated record set related to treatment, payment and health care operations.

\textsuperscript{5} It is important to note, however, that OCR has maintained the requirements that covered entities maintain for six years (1) a copy of any accounting provided to an individual, and (2) the titles of the persons or offices responsible for receiving and processing requests for such accountings, from the date of creation or the date last in effect, whichever is later.

\textsuperscript{6} 45 C.F.R. § 164.400 et seq.

\textsuperscript{7} This includes disclosures (1) to the individuals of their own PHI; (2) incident to a permitted use or disclosure; (3) pursuant to an authorization; (4) for facility directories; (5) for national security or intelligence purposes; (6) to correctional institutions or law enforcement officials (with respect to certain disclosures); (7) of limited data sets; and (8) occurring before the compliance date for the covered entity.
OCR also proposes to exclude additional disclosures from the accounting requirement, and requests comment on such exemptions. These exclusions are:

- disclosures related to reports of adult abuse, neglect or domestic violence, because of concerns that such disclosure may endanger the reporter;
- disclosures for research in which individual authorization has been waived under the Privacy Rule, because of the potential administrative burden it places on health systems and health services research;
- disclosures for health oversight activities, because such disclosures relate to the covered entity, rather than the individual;
- disclosures about decedents to coroners, medical examiners and funeral directors, because they are routine, expected and do not raise significant privacy concerns;
- disclosures for cadaveric organ, eye or tissue donation purposes, because families would be involved in the decision process with respect to such donations;
- disclosures for protective services for the President and others; and
- most disclosures required by law, because they represent a determination by a governmental body that such disclosure should be made and accounting for such nondiscretionary disclosures imposes a significant burden on covered entities. 8

- **Modify the accounting content requirements.**

The current Privacy Rule requires an accounting of disclosures to contain the date of disclosure, name and (if known) address of the recipient, a brief description of the type of PHI disclosed, and a brief statement of the purpose of the disclosure. OCR proposes to modify these content requirements.

First, OCR proposes to require the covered entity (or business associate) to provide only an approximate date or period of time for each disclosure, if the actual date is unknown. The approximate date must include a month and year or a description of when the disclosure occurred so that the individual can readily determine the approximate month and year of the disclosure. Under the proposed rule, the approximate timeframe would suffice in the event of multiple disclosures to the same person or entity for the same purpose, but not for a single disclosure. OCR would also permit the date of disclosure to be descriptive (e.g., “within 15 days of discharge” or “the fifth day of the month following discharge”).

Second, while the name of the entity or natural person receiving the PHI must be included in the accounting, OCR proposes to exempt such information when the name of the recipient of PHI provided in the accounting would itself represent a disclosure of PHI about another individual (e.g., an individual’s appointment reminder is sent to another patient.)

Third, OCR also proposes a minor change to the language regarding the description of the PHI disclosed and the purpose of disclosure. OCR proposes to replace “a brief description of the protected health information disclosed” with “a brief description of the type of protected health information disclosed.”

---

8 OCR requests comment on whether there are other categories of public health disclosures that may also warrant exemption because they would be of limited interest to individuals or because accounting for such disclosures may adversely affect the public health activity.
Fourth, OCR also proposes to slightly revise the language regarding the purpose of disclosure. It proposes to change the current language from “statement” to “description,” so that it is clear that a minimum description is sufficient if it reasonably informs the individual of the purpose.

Finally, OCR proposes to require covered entities to give individuals the option to limit the accounting request to a particular time period, type of disclosure or recipient. Covered entities may also offer additional options to individuals for limiting an accounting request (e.g., limit to a specific organization).

- Establish requirements for the provision of an accounting of disclosures.

OCR proposes revisions to the requirements on how an accounting of disclosures is provided, such as the timeframe for providing an accounting, the form of the request and permissible charges for an accounting. OCR proposes three modifications to the existing Privacy Rule requirements: (1) to decrease the permissible response time from 60 days to 30 days (with an additional 30-day extension, as currently permitted); (2) to require covered entities to provide individuals with the accounting in the form (paper or electronic) and format (e.g., a particular software application) requested by the individual, if readily producible in such form and format; and (3) to clarify that the covered entity may require the individual to submit the request in writing. Under the proposed rule, OCR would continue to prohibit covered entities from charging individuals for the first request for an accounting in a 12-month period, but permit reasonable, cost-based charges for subsequent accounting requests; the covered entity would be required to inform the individual at the time of the first request and of the subsequent request that such subsequent requests may be subject to a fee (and permit the individual to withdraw or modify such subsequent request to avoid or reduce the fee).

Under the proposed rule, covered entities would continue to be able to delay provision of an accounting due to an ongoing law enforcement investigation. As clarification, if a law enforcement investigation delays an accounting, OCR proposes to require the covered entity to provide an accounting of other disclosures and to supplement the accounting with information about the law enforcement disclosure at the conclusion of the delay. OCR also proposes to eliminate the currently permitted delay of an accounting response for health oversight investigations since it proposes to eliminate the requirement to account for health oversight disclosures.

- Revise accounting of disclosures documentation requirements.

OCR proposes to revise the documentation requirements for accounting of disclosures. Under the current Privacy Rule, a covered entity must maintain documentation to provide an accounting of disclosures for six years. The covered entity must also maintain the written accounting that it provided and the designation of the person or offices responsible for receiving and processing accounting requests. OCR proposes two changes to these requirements: (1) to require covered entities to maintain documentation necessary to provide an accounting of disclosures for three years (since the accounting period is reduced from six to three years) and (2) to revise the regulation to clarify that a covered entity must retain a copy of the accounting provided to the individual, not the original accounting document itself.  

---

9 As noted above, the copy of the written accounting and the designation of the person or office responsible for receiving and processing accounting requests must still be maintained for six years.
Access Report – Section 164.528(b)

To meet requirements in HITECH Act § 13405(c), OCR proposes to provide individuals with a right to receive an access report that serves to document who has accessed an individual’s electronic designated record set information. The proposed rule expands this right (1) to all uses and disclosures, rather than only disclosures, including disclosures for treatment, payment and health care operations, and (2) to all electronic PHI in a designated record set, rather than only in an EHR. OCR believes this expansion will increase the benefits to individuals by giving them more information on who has accessed their electronic PHI. OCR also believes that limiting the access report to electronic information in a designated record set will limit the administrative burden on covered entities.

The proposal extends the right to an access report to all covered entities and business associates that maintain electronic designated record set information, rather than only those covered entities that maintain PHI in an EHR. OCR believes that the administrative burden of the proposed rule will be reasonable due to the obligation under the HIPAA Security Rule of all covered entities to log electronic PHI access information.

Under the proposed rule, a covered entity would include in its access report information from business associates that handle designated record set information, rather than providing an individual with a list of business associates (as provided in the HITECH Act).

- Contents of the Access Report

OCR proposes that the access report contain (a) the date of the access; (b) the time of access; (c) the name of the natural person (if available), or otherwise the name of the entity, that accesses the electronic designated record set information; (d) description of what information was accessed, if available; and (e) a description of the action by the user, if available (e.g., create, modify, delete). Unlike an accounting for disclosure, an access report would not include the address of the user or a brief statement of the purpose of the disclosure because this information is generally not collected in an access log.

OCR believes that the proposed access report right will require minimal changes to a covered entity or business associate’s existing information systems. It notes that entities that are in compliance with the Security Rule should already be logging the information necessary to generate such an access report. OCR acknowledges that the information necessary to generate an access report may be in separate systems and that it may pose a significant burden to aggregate the information into one report, but it believes that the administrative burden is reasonable in light of the individual’s interest in knowing who has accessed the electronic PHI used to make decisions about him or her.

OCR also proposes to require covered entities to provide individuals with an option to limit the access report to a specific date, time period or person. This option would allow an individual to focus his/her request and reduce the burden on covered entities. OCR is recommending, but not requiring, covered entities to offer individuals an option to limit an access report to access made by a specific organization. OCR proposes that access reports be provided to the requesting individual in a format that is understandable to him or her without external aid.
• Provision of the Access Report

OCR proposes the same timing requirement for the provision of an access report as is proposed for an accounting of disclosures. Under the proposal rule, a covered entity would have 30 days to provide an access report. The response period may be extended once for a 30-day period when necessary. The proposed rule requires the covered entity to provide the access report in the form and format requested by the individual, if it is readily producible in the requested form and format. The covered entity may not charge an individual for providing the first access report in a 12-month period, but may charge a fee for subsequent access report request during the 12-month period. The individual must be provided, at the time of the first request and of the subsequent request, with notice that such subsequent requests may be subject to a fee (and permit the individual to withdraw or modify such subsequent request to avoid or reduce the fee). Additionally, the covered entity may require an individual to make access report requests in writing, if it informs the individual of the written request requirement. OCR encourages covered entities to create forms for individuals to use to request an access report.

• Documentation

The proposed documentation requirement for access reports is the same as for accountings for disclosures. Covered entities and business associates would have to retain documentation needed to produce an access report for three years. The covered entity must retain for six years copies of access reports that were provided to individuals and must maintain a designation of the persons or offices responsible for receiving and processing requests for access reports for six years.

Accounting for Treatment, Payment & Health Care Operations Disclosures through Electronic Information Exchange – and Confidentiality of Patient Safety Work Product

OCR notes that it considered providing individuals with the right to receive a full accounting of treatment, payment and health care operations disclosures through an EHR when such EHR disclosures are received by another electronic system. It concluded that, at the present time, such an accounting would be overly burdensome to covered entities when compared to the potential benefit to the individual. OCR notes, however, that it intends to work with the Office of the National Coordinator for Health Information Technology to assess whether, as standards for electronic health exchange are adopted, the standards should include information about the purpose of each exchange transaction. When that happens, OCR intends to revisit the issue and consider whether to revise the accounting requirements to include a requirement to account for disclosures for treatment, payment and/or health care operations.

OCR also proposes to exclude from both the requirement to account for disclosures and from the requirement to provide access reports information that meets the definition of patient safety work product at 42 C.F.R. § 3.20, because the disclosure that electronic PHI was disclosed or accessed for such patient safety purposes may itself reveal patient safety work product.
Notice of Privacy Practices – Section 164.520

The current Privacy Rule requires a covered entity to provide individuals with a notice of its privacy practices. The notice must include descriptions of the individual’s rights under the Privacy Rule, including the right to obtain an accounting of disclosures.

OCR proposes to revise the requirement to include a statement of the individual’s right to obtain an access report. OCR notes that this proposed change to the notice of privacy practices would constitute a material change to the notice. Under the Privacy Rule, a covered entity would be required to promptly revise and distribute the notice, as outlined in section 164.520(c), when the change becomes effective.

For more information on the proposed rule or to discuss the potential impact of the proposed rule on your organization, please do not hesitate to contact a member of the Alston & Bird Health Care Regulatory Group.
If you would like to receive future Health Care Advisories electronically, please forward your contact information including e-mail address to healthcare.advisory@alston.com. Be sure to put “subscribe” in the subject line.

For further information, please do not hesitate to contact any of the following:

**Atlanta Office**

- Donna P. Bergeson
  - 404.881.7278
  - donna.bergeson@alston.com
- Edward P. Bonapfel
  - 404.881.7166
  - ed.bonapfel@alston.com
- Angela T. Burnett
  - 404.881.7665
  - angie.burnett@alston.com
- John R. Hickman
  - 404.881.7685
  - john.hickman@alston.com
- Sean C. Hyatt
  - 404.881.4410
  - sean.hyatt@alston.com
- William H. Jordan
  - 404.881.7850
  - bill.jordan@alston.com
- Robert C. Lower
  - 404.881.7455
  - bob.lower@alston.com
- Dawnmarie R. Matlock
  - 404.881.4253
  - dawnmarie.matlock@alston.com
- Kim McWhorter
  - 404.881.4254
  - kim.mcwhorter@alston.com
- D’Andrea J. Morning
  - 404.881.7538
  - dandrea.morning@alston.com
- Robert D. Stone
  - 404.881.7270
  - robert.stone@alston.com
- Michelle A. Williams
  - 404.881.7594
  - michelle.williams@alston.com
- Esther Yu
  - 404.881.4240
  - esther.yu@alston.com

**Washington Office**

- Jennifer L. Butler
  - 202.756.3326
  - jennifer.butler@alston.com
- Joyce E. Gresko
  - 202.239.3628
  - joyce.gresko@alston.com
- Elinor A. Hiller
  - 202.239.3401
  - elinor.hiller@alston.com
- Peter M. Kazon
  - 202.756.3334
  - peter.kazon@alston.com
- Stephanie A. Kennan
  - Senior Public Policy Advisor
  - 202.756.3159
  - stephanie.kennan@alston.com
- Keavney F. Klein
  - 202.239.3981
  - keavney.klein@alston.com
- Rudy S. Missmar
  - 202.756.3034
  - rudy.missmar@alston.com
- Michael H. Park
  - 202.239.3630
  - michael.park@alston.com
- Earl Pomeroy
  - Senior Counsel
  - 202.239.3835
  - earl.pomeroy@alston.com
- Mark Rayder
  - Senior Public Policy Advisor
  - 202.756.3562
  - mark.rayder@alston.com
- Colin T. Roskey
  - 202.756.3436
  - colin.roskey@alston.com
- Marc J. Scheineson
  - 202.756.3465
  - marc.scheineson@alston.com
- Thomas A. Scully
  - 202.756.3459
  - thomas.scully@alston.com
- Donald E. Segal
  - 202.756.3449
  - donald.segal@alston.com
- Robert G. Siggins
  - Senior Policy Advisor
  - 202.239.3836
  - bob.siggins@alston.com
- Paula M. Stannard
  - 202.756.3489
  - paula.stannard@alston.com
- Tamara R. Tenney
  - 202.756.3489
  - tamara.tenney@alston.com
- Julie K. Tibbets
  - 202.756.3444
  - julie.tibbets@alston.com
- Timothy P. Trysla
  - 202.756.3420
  - tim.trysla@alston.com
- Marilyn Yager
  - 202.756.3341
  - marilyn.yager@alston.com

**ATLANTA**

One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404.881.7000

**CHARLOTTE**

Bank of America Plaza
Suite 4000
101 South Tryon Street
Charlotte, NC 28280-4000
704.444.1000

**DALLAS**

Chase Tower
Suite 3601
2200 Ross Avenue
Dallas TX 75201
214.922.3400

**LOS ANGELES**

333 South Hope Street
16th Floor
Los Angeles, CA 90071-3004
213.576.1000

**NEW YORK**

90 Park Avenue
New York, NY 10016-1387
212.210.9400

**RESEARCH TRIANGLE**

4721 Emperor Boulevard
Suite 400
Durham, NC 27703-8580
919.862.2200

**SILICON VALLEY**

275 Middlefield Road
Suite 150
Menlo Park, CA 94025-4004
650.838.2000

**VENTURA COUNTY**

Suite 215
2801 Townsgate Road
Westlake Village, CA 91361
805.497.9474

**WASHINGTON, D.C.**

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202.239.3300

www.alston.com
© Alston & Bird LLP 2011