Connecting Healthcare with Legal Excellence℠

Health Law Diagnosis

HIPAA ACCOUNTING OF DISCLOSURES: PROPOSED NOTICE OF RULEMAKING

On Friday, May 27, the Department of Health and Human Services (HHS) issued a **notice of proposed rulemaking ("Proposed Rule")** to modify the HIPAA Privacy Rule in order to implement the HITECH accounting requirement.[1] Over 170 comments were received in response to the request for information published by HHS on May 3, 2010. The Proposed Rule:

- Splits the current accounting provision of the Privacy Rule, § 164.528, into two separate rights: (a) **right to receive an accounting**; and (b) **right to receive an access report**;
- Extends both accountings and access reports to *information maintained within a designated record set,* not just TPO disclosures through an electronic health record (EHR);
- Makes the information in such designated record sets available to an individual for both rights within a *3 year period* instead of six as currently set forth by the accounting requirements;
- Requires for an *accounting of disclosures* the provision of information about the disclosure of information in the designated record set, *hard copy or electronic*, to persons outside of the covered entity or business associate, for specific purposes, such as law enforcement, public health investigations, or judicial hearings;
- Requires for an *access report* information regarding all *electronic accesses* by covered entity and business associate workforce members as well as outside persons of the individual's *electronic PHI maintained in an electronic designated record set*; and
- Requires modification of Notice of Privacy Practices to include new right to access reports and modification of accounting of disclosures right.

[1] The HIPAA Privacy Rule at Section 45 CFR 164.528 requires an accounting of certain disclosures ("Accounting") of an individual's PHI to be made available to an individual upon request for the six (6) years prior to the date of the request. Section 164.528(a)(1) currently provides that an accounting must include all disclosures of protected health information, **except for** disclosures: (i) to carry out treatment, payment and health care operations as provided in §164.506; (ii) to individuals of protected health information about them as provided in §164.502; (iii) incident to a use or disclosure otherwise permitted or required by this subpart, as provided in §164.502; (iv) pursuant to an authorization as provided in §164.508; (v) for the facility's directory or to persons involved in the individual's care or other notification purposes as provided in §164.510; (vi) for national security or intelligence purposes as provided in §164.512(k)(2); (vii) to correctional institutions or law enforcement officials as provided in §164.512(k)(5); (viii) as part of a limited data set in accordance with §164.514(e); or, (ix) that occurred prior to the compliance date for the covered entity. Section 13405(c) of the Health Information Technology for Economic and Clinical Health Act ("HITECH") removed the TPO exemption where the disclosures are made through "an electronic health record." For any TPO disclosures made by a business associate through an EHR, the covered entity could either provide an accounting of the business associate's disclosures, or provide a list with the contact information of all business associates that the individual can contact to receive an accounting of such business associate's TPO disclosures.

Accounting of Disclosures

In general, an individual would continue to have a right to receive an accounting of certain disclosures under the Privacy Rule. The Proposed Rule would change the scope of information that would be subject to the accounting, explicitly including disclosures made to or by business associates, changing the accounting period from **six (6) years to three (3) years,** and would list the information *subject* to the accounting instead of those disclosures *exempt* from the accounting. The Proposed Rule would further limit the information that would be made available to that information maintained in a designated record set (DRS). Because covered entities are already required to document DRS subject to access by individuals, the Proposed Rule states that covered entities are therefore more easily capable of tracking any disclosures of PHI through these defined and established record sets and systems.

Although covered entities would continue to be required to account for impermissible disclosures, any disclosures that a covered entity has already made an individual aware of as required by the HITECH Breach Notification Rule would be exempt. The Proposed Rule would continue to include in the accounting:

- Disclosures for public health activities (except reports of child abuse or neglect);
- Judicial and administrative proceedings (even if required by law);
- Law enforcement activities (even if required by law);
- To avert a serious threat to health or safety;
- Military and veterans' activities;
- Department of State's medical suitability:
- Government programs providing public benefits; and
- Workers' compensation.

It would also retain the current exemptions to the accounting requirement under the Privacy Rule. Disclosures for TPO, in particular, would continue to be exempt for paper records, but would be included for purposes of the proposed provision of access reports, as described below. Furthermore, the Proposed Rule would **exclude** from accountings disclosures concerning:

- Victims of abuse, neglect or domestic violence;
- Health oversight activities;
- Research purposes;
- Decedents to coroners, medical examiners, and funeral directors;
- Cadaveric organ, eye or tissue donation purposes;
- Disclosures for protective services for the President and others; and
- Disclosures required by law.

As noted above, disclosures which would be exempt from the accounting requirement would be made available to an individual to the extent they are made through direct access to electronic designated record set information through an access report, as described below, even though such information may not be identified.

The content of the accounting would remain generally the same; i.e., the date of disclosure, name and (if known) address of the recipient, brief description of the *type* of PHI disclosed, and brief description of the purpose. However, the Proposed Rule, would require *only* an approximate date or period of time for each disclosure, if the actual date was not known, which at a minimum would need to include the month and year, or a description of when the disclosure occurred from which an individual can "readily determine" the month and year of the disclosure. It would also permit a descriptive date (e.g., within 15 days of discharge). In addition, for multiple disclosures for the same purpose, the Proposed Rule would find the approximate period of time to be sufficient, and would not require an exact start and end date. The Proposed Rule also set forth the following additional changes:

- Individual can limit the accounting to a particular time period, type of disclosure or recipient;
- *30 day response* timeframe, instead of 60 days, with additional 30 day extension;
- Provision of the accounting in the ***form and format requested by the individual*** if readily producible in that format; if not readily producible, provision in hard copy or work with individual to provide in another form and format;
- Clarification of the *reasonable and appropriate safeguards* which must be in place to deliver a copy of the accounting to the individual. Therefore, if an individual requests an electronic copy of the accounting but not does want the file encrypted, a covered entity may provide the copy without such encryption;
- Underlying documentation with accounting only needs to be maintained for a **3-year** period;
- Retention of only a copy of the accounting provided to the individual, not the original accounting document, for six (6) years from the date on which the accounting was provided; and
- Exclusion from accounting any information that meets the definition of patient safety work product at 42 CFR 3.20.

Access Report

The Proposed Rule would create a separate right of an individual to receive an access report which identifies who has had access to their information maintained in an electronic DRS. The access report would capture *all accesses* to an *electronic DRS*, whether by a member of the covered entity's workforce or by an outside third-party. It would not distinguish between uses or disclosures, thereby resolving an issue identified by many commenters. It would identify the date, time and name of the person or entity accessing the information, as well as a description of the information accessed and any actions performed to the extent such information is available. Covered entities would be required to include within their **Notice of Privacy Practices** a statement informing individuals of their right to receive an access report in addition to their right to receive an accounting of certain disclosures.

The Proposed Rule would require covered entity access logs to collect raw data from the electronic system containing PHI each time a user accesses information. The access report would be generated from the access log in a format that is understandable to the individual. The Preamble to the Proposed Rule notes that separate access logs would be maintained by the

multiple systems which have electronic DRS and that HHS' expectation would be that the data from each access log would be gathered and aggregated to generate *one single access report*. Although HITECH references only disclosures made through an EHR for TPO, the HHS notes in the Preamble that it has exercised its general discretion and proposes to broaden this right to all *"uses"* of information as well as to *all electronic PHI maintained in a* DRS, rejecting the need to categorize certain electronic systems as EHRs. Therefore, only information accessed and disclosed through an electronic DRS will be captured and provided to an individual through the access report.

Covered Entities are responsible for collecting access reports from their respective business associates that maintain DRS information. Under the current requirements of the Security Rule applicable to business associates, business associates should be able to generate access reports indicating who has access the individual's electronic DRS information. Although permissible under the accounting requirement, the covered entity could not provide a list and contact information of all of its business associates who maintain the individual's information in a DRS. As such, the covered entity is responsible for contacting applicable business associates to obtain access reports from them which it would in turn incorporate into its single access report to provide to the individual.

The Proposed Rule would require the **access report** to set forth the following information:

- Date and time of access (at least start time, and free to include end time);
- Name of the person, if available, or entity accessing the electronic DRS (must readily match a user ID with a first and last name, or the organization's name receiving the information);
- Description of what information was accessed, if available; and
- Description of the action taken by the user, if available (e.g., "create", "modify", "access" or "delete").

The Proposed Rule specifically would not require a description of the purpose of the disclosure, such to whom the user provided the information or for what purpose its use or disclosure was for. The Preamble specifically states that the burden on covered entities significantly outweighs the benefit to individuals of learning of such purpose, as not only existing systems but workflow as well would need to be extensively modified at significant time and cost. The Preamble notes that it does not proposed inclusion of the ultimate recipient, unless such recipient would be the person with direct access to the electronic PHI, as such information is not currently available in systems.

Much like for the accounting, the Proposed Rule would require the access report to include only information within a three-year period from the date of the request. Additionally, much like the accounting, the covered entity would be required to give the individual the option of limiting the access report to a specific time period, date or person, and covered entities would also be encouraged to limit the report to specific organizations. A reasonable cost-based fee would be permitted beyond the first access report provided within a 2-month period and the covered entity could require any request for an access report to be in writing, as they are permitted to do with accounting requests. The Proposed Rule would also require the following changes:

- *30 day response* timeframe, with 30 day extension;

- Provision of the report in a format *understandable to the individual* (e.g., reasonably understood without an external aid) such as:

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

- Provision of the accounting in a *machine readable (e.g., Word, Excel) or other electronic form and format requested by the individual if readily producible in that format;* if not readily producible, in a *readable electronic form and format* as agreed to by the covered entity and the individual. If the individual does not agree to the readable electronic format readily producible, or if the individual so requests, the covered entity may provide a readable hard copy;

- Documentation of information required to produce an access report only needs to be maintained for a **3-year period;**

- Retention of only a copy of the access report provided to the individual, not the original document, for six (6) years from the date on which the report was provided;

- Exclusion from access report any information that meets the definition of patient safety work product at 42 CFR 3.20.

Notice of Privacy Practices

The Proposed Rule would require covered entities to include in their Notice of Privacy Practices statements that individuals are accorded both the right to receive an accounting of disclosures and a right to receive an access report. Because the right to an access report would be considered a material change to the notice, as specifically noted in the Preamble to the Proposed Rule, covered entities would be required to revise and distribute the notice as required by § 164.520(b) and (c).

However, because the effective dates for compliance with the access report requirements is not until at least 2013 for certain covered entities, such revision and distribution would not be required until the earliest applicable compliance date. Unlike the right to access reports, the Preamble to the Proposed Rule notably does not specifically state that the changes to the accounting requirement are material changes; as such, although the notice will need to be revised to set forth the modified accounting requirements (e.g., within a three (3) year period only), *it will not need to be distributed to individuals until it is revised and distributed as required by the applicable effective compliance date for access reports.*

Health Information Exchanges

The Preamble to the Proposed Rule notes that it considered, but rejected, a full accounting of disclosures for TPO that are made through a health information exchange at this time, which would have included a *full description* of the purpose of the disclosure; however, HHS states in the Preamble its intentions to work with ONC to assess whether standards for exchanges of information should include information about the purpose of each transaction. To the extent such information would fall under a disclosure required to be accounted for (e.g., public health), the individual would still have a right to learn of such a disclosure. Furthermore, each access to any electronic DRS information for purposes of an electronic HIE would additionally be captured in the access report (e.g., date, time, identity of user). Therefore, for purposes of fulfilling their obligations as business associates of their participants, HIEs will remain responsible for providing information required in order for a participant to respond to an individual's request for an accounting, as well as access reports under the current and Proposed Rule.

The compliance deadline for the new accounting requirements would be 180 days after the effective date of the final regulation (240 days after publication). An individual would need to be provided with the right to an access report beginning January 1, 2013 for electronic DRS systems acquired after January 1, 2009, and beginning January 1, 2014, for electronic DRS systems acquired as of January 1, 2009. Thus, a covered entity may be responsible for producing access reports from some systems, but not all, during 2013, depending upon when each DRS system was acquired.

A full copy of the Proposed Rule can be located at http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf. **Public comments were due by August 1, 2011**.

* * * *

For more information, please contact:

Helen Oscislawski, Esq.
Principal at Oscislawski LLC
tel: 609-385-0833, ext. 1
helen@oscislaw.com

OR

Krystyna Monticello, Esq.
Partner at Oscislawski LLC
tel: 609-385-0833, ext. 2
kmonticello@oscislaw.com

Attorneys at Oscislawski LLC is a health law firm with its main office located in Princeton, New Jersey but a nationwide reputation for experience with and understanding of federal and state privacy and security laws, as well as electronic health information exchange, health information technology, and managing health data breaches. Our attorneys also advise clients on wide-range of other legal issues. For more information about our firm visit www.oscislaw.com. ***For excellent compliance information, tools and solutions, please also visit our affiliated blog & resource website*** *www.legalhie.com.*