



HEALTH LAW REPORTER



Reproduced with permission from BNA's Health Law Reporter, 24 HLR 921, 6/16/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

HHS Proposed Rule Creates New Access Report Obligations And Amends Existing Accounting of Disclosures Provisions



BY REECE HIRSCH AND HEATHER DEIXLER

On May 31, the Department of Health and Human Services (HHS) released a notice of proposed rulemaking (the proposed rule) creating a new requirement that covered entities produce an “access report” informing individuals of those who have viewed their records, while also modifying existing accounting of disclosures rules under the Health Insurance and

Reece Hirsch is a partner in the San Francisco office of Morgan, Lewis & Bockius LLP and can be reached at (415) 442-1422 or rhirsch@morganlewis.com. Heather Deixler is an associate in the San Francisco office of Morgan Lewis and can be reached at (415) 442-1317 or hdeixler@morganlewis.com.

Portability and Accountability Act of 1996 (HIPAA).¹ The proposed rule would impose significant new obligations on all HIPAA-covered entities, including health care providers and health plans.

The proposed rule was issued, in part, to implement the statutory requirements of the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). However, HHS continues to demonstrate its willingness to utilize the rulemaking process to go beyond the statutory provisions of the HITECH Act, introducing significant modifications to existing HIPAA standards (the accounting of disclosure requirements) and entirely new obligations (the access report requirements).

The HITECH Act contained a requirement that covered entities provide an accounting of disclosures from an electronic health record (EHR) to carry out treatment, payment and health care operations.² On May 3, 2010, HHS published a request for information (RFI) relating to this new standard. HHS notes that “a large percentage” of the comments in response to the RFI expressed concerns that the new accounting of disclosures requirement would increase health care costs, reduce patient care time due to disruptions in provider workflow and have a potential chilling effect on the adoption of EHR systems, particularly for small provid-

¹ “HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act,” 76 Federal Register 31426 (May 31, 2011). Available at <http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf>.

² American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009), at § 13405(c)(1)(A).

ers.³ In the proposed rule, HHS appears to have attempted to respond to such concerns by modifying the existing accounting of disclosures standard, but health care industry commenters will be considering the extent to which the modifications impose new burdens on covered entities.

Covered entities would be required to provide access reports commencing Jan. 1, 2013 (for electronic designated record set systems acquired after Jan. 1, 2009) and Jan. 1, 2014 (for electronic designated record set systems acquired on or before Jan. 1, 2009). Covered entities would be required to comply with the new accounting of disclosures requirements beginning 240 days after publication of the final regulations. HHS is accepting comments on the proposed rule through Aug. 1.

Accounting of Disclosures of Protected Health Information

Right to an Accounting of Disclosures

Under Section 164.528(a)(1)(i) of the proposed rule, an individual would retain the right to receive an accounting of disclosures from a covered entity, but this right would be modified in several ways.

First, the scope of the individual's information subject to the accounting would be limited to information contained in a designated record set.⁴ A designated record set includes the medical and health care payment records maintained by or for a covered entity, as well as other records used by or for the covered entity to make decisions about individuals.⁵ Under the HIPAA Standards for Privacy of Individually Identifiable Health Information (the privacy rule), an individual currently has a right to an accounting of certain disclosures of PHI about the individual, regardless of where such information is located. In the preamble to the proposed rule, HHS maintains that limiting the information subject to an accounting would better align the accounting provision with an individual's rights to access and amend PHI under Sections 164.524 and 164.526 of the privacy rule, both of which are limited to PHI contained in a designated record set. In other words, by limiting the accounting to the information contained in a designated record set, which equates to the information that "forms the basis for covered entities' health care and payment decisions about the individual," the accounting will contain the "protected health information that is of most interest to the individual."⁶

Second, the proposed rule would include a direct reference to business associates in the standard, clarifying that the covered entity now is responsible for including all disclosures by its business associates that create, receive, maintain or transmit designated record set information.⁷ While the privacy rule currently requires covered entities to ensure that their business associates *make available* the information required to provide an accounting of disclosures, the proposed rule would go a step further to actually require the covered entity to in-

clude the disclosures of its business associates in the accounting. As with the accountings for covered entities, business associates' accountings also would be limited to information contained in their designated record sets.

Third, the proposed rule would reduce the accounting period to disclosures occurring during the previous three years, rather than six years, as currently required under the privacy rule.⁸ In an effort to achieve a consistent approach, the proposed rule would adopt the three-year standard set forth in the HITECH Act with respect to accounting of disclosures from EHRs.⁹ HHS states that this more limited timeframe would not significantly disadvantage individuals, since those seeking an accounting of disclosures tend to be most interested in learning of recent disclosures.¹⁰ If a covered entity has been subject to the privacy rule for less than three years, the covered entity would only need to account for the period of time during which the entity was subject to the privacy rule.¹¹

Fourth, the proposed rule would provide a list of the types of disclosures subject to the accounting, in contrast to the current requirement that disclosures be included in an accounting, subject to the availability of specified exceptions.¹² The proposed rule also would continue to require covered entities to account for disclosures that are impermissible under the privacy rule, unless the disclosure constitutes a breach within the meaning of the HITECH Act security breach notification regulations (the breach notification rule).¹³ HHS believes that it is not necessary to require covered entities to account for disclosures associated with a breach for which the individual has already received written notification under the breach notification rule.¹⁴

HHS has proposed to continue to include the following disclosures in the accounting requirements: disclosures for public health activities (except those involving reports of child abuse or neglect), for judicial and administrative proceedings, for law enforcement activities, to avert a serious threat to health or safety, for military and veterans activities, for the Department of State's medical suitability determinations, to government programs providing public benefits and for workers' compensation.¹⁵

In the proposed rule, HHS is considering exempting disclosures for research purposes from the accounting requirement.¹⁶ Even though current privacy rule requirements include a simplified accounting option for research disclosures with respect to large studies, HHS is attempting to respond to concerns from the research community that the administrative burden of the accounting requirements has a potentially chilling effect on human subjects research.¹⁷ The proposed rule also would exempt from the accounting requirement disclo-

⁸ *Id.*

⁹ 76 Fed. Reg. at 31430.

¹⁰ *Id.*

¹¹ 76 Fed. Reg. at 31434.

¹² 76 Fed. Reg. at 31430-31 (to be codified at 45 C.F.R. § 164.528(a)(1)(i)).

¹³ 76 Fed. Reg. at 31431 (to be codified at 45 C.F.R. § 164.528(a)(1)(i)(A)).

¹⁴ 76 Fed. Reg. at 31431.

¹⁵ 76 Fed. Reg. at 31431 (to be codified at 45 C.F.R. § 164.528(a)(1)(i)(B)-(G)).

¹⁶ 76 Fed. Reg. at 31432.

¹⁷ *Id.*

³ 76 Fed. Reg. at 31428.

⁴ 76 Fed. Reg. at 31430 (to be codified at 45 C.F.R. § 164.528(a)(1)(i)).

⁵ 45 C.F.R. § 164.501.

⁶ 76 Fed. Reg. at 31430 (to be codified at 45 C.F.R. § 164.528(a)(1)(i)).

⁷ *Id.*

tures (i) for health oversight activities, (ii) to coroners, medical examiners and funeral directors and (iii) required by law.¹⁸

Content of the Accounting

The proposed rule would modify certain elements of the existing content requirements for an accounting of disclosures. Under the privacy rule, an accounting must contain: (i) the date of disclosure; (ii) name and (if known) address of the recipient; (iii) a brief description of the type of PHI disclosed; and (iv) a brief statement of the purpose of the disclosure. Under the proposed rule, an accounting need not include a specific date of disclosure, but could include an approximate time range, or even a descriptive date of disclosure, where the actual date was not known.¹⁹ The proposed rule would require an explanation of the type of PHI disclosed, instead of a brief description of the PHI disclosed, reflecting that the accounting is focused on the types of PHI that were the subject of the disclosure.²⁰ The proposed rule also would require a *description* of the purpose, instead of a *statement* of the purpose, in an effort to clarify that only a “minimum description is required if it reasonably informs the individual of the purpose.”²¹ Perhaps most significantly, the proposed rule also would give individuals the option to limit their accounting to either a particular time period, type of disclosure or recipient.²²

Provision of Accounting

The proposed rule would make the following changes to the requirements relating to the provision of an accounting of disclosures:

- decrease the timeframe for responding to an accounting request to 30 days, rather than 60 days;²³
- require that covered entities provide individuals with the accounting in the form (e.g., paper or electronic) and format (i.e., compatible with a specific software application) requested by the individual, if readily producible;²⁴ and
- clarify that the covered entity may require the individual to submit the accounting request in writing (which includes electronic requests), provided that the covered entity informs individuals of this requirement.²⁵

If the covered entity is unable to provide the accounting within 30 days, the covered entity may extend the period by no more than 30 days, so long as the individual receives a written statement of the reasons for

the delay and the date by which the covered entity will provide the accounting.²⁶

The proposed rule would maintain the current requirement that a covered entity not charge for the first request for an accounting during a 12-month period, but may charge a reasonable and cost-based fee for any subsequent requests during the 12-month period. The covered entity would, however, be required to inform the individual of the fee at the time of the subsequent request and would need to provide the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.²⁷

Documentation

The proposed rule would modify current documentation requirements under the privacy rule to require a covered entity to retain:

- documentation needed to generate an accounting of disclosures for three years (rather than for six years, as required by the privacy rule);²⁸
- a copy of the actual accounting that was provided to an individual for six years from the date the accounting was provided;²⁹ and
- documentation designating the individual responsible for handling accounting requests for six years from the last date the designation was in effect.³⁰

Access Reports

Right to an Access Report

Under Section 164.528(b)(1) of the proposed rule, covered entities would be required to provide an individual with an “access report” identifying who has accessed the individual’s electronic designated record set information. This new access right does not extend to paper records.³¹

The new access right is based in part on a requirement established by the HITECH Act providing individuals with an accounting of disclosures through an EHR for treatment, payment and health care operations. The proposed rule varies from the HITECH Act provision in two significant ways:

- o First, the proposed rule provides an individual with the right to be informed of all persons who have accessed their record, regardless of whether the information was actually *disclosed* to someone outside of the covered entity’s workforce.³²
- o Second, while the HITECH Act provided for accounting of disclosures from EHRs, the proposed rule creates a new right to receive an access report with respect to the designated record set maintained by all covered entities, regardless of whether those entities have implemented EHRs.³³

¹⁸ 76 Fed. Reg. at 31433.

¹⁹ 76 Fed. Reg. at 31434 (to be codified at 45 C.F.R. § 164.528(a)(2)(i)(A)(1)).

²⁰ 76 Fed. Reg. at 31434 (to be codified at 45 C.F.R. § 164.528(a)(2)(i)(C)).

²¹ 76 Fed. Reg. at 31434 (to be codified at 45 C.F.R. § 164.528(a)(2)(i)(D)).

²² 76 Fed. Reg. at 31434 (to be codified at 45 C.F.R. § 164.528(a)(2)(ii)).

²³ 76 Fed. Reg. at 31435 (to be codified at 45 C.F.R. § 164.528(a)(3)(i)).

²⁴ 76 Fed. Reg. at 31435 (to be codified at 45 C.F.R. § 164.528(a)(3)(ii)).

²⁵ 76 Fed. Reg. at 31435 (to be codified at 45 C.F.R. § 164.528(a)(3)(iv)).

²⁶ 76 Fed. Reg. at 31435 (to be codified at 45 C.F.R. § 164.528(a)(3)(i)(B)(1)-(2)).

²⁷ 76 Fed. Reg. at 31435 (to be codified at 45 C.F.R. § 164.528(a)(3)(iii)(B)).

²⁸ 76 Fed. Reg. at 31436 (to be codified at 45 C.F.R. § 164.528(a)(5)(i)).

²⁹ 76 Fed. Reg. at 31436 (to be codified at 45 C.F.R. § 164.528(a)(5)(ii)(A)).

³⁰ 76 Fed. Reg. at 31436 (to be codified at 45 C.F.R. § 164.528(a)(5)(ii)(B)).

³¹ 76 Fed. Reg. at 31436 (to be codified at 45 C.F.R. § 164.528(b)(1)).

³² 76 Fed. Reg. at 31436.

³³ *Id.*

HHS maintains that this new access right would not impose an unreasonable burden on covered entities because, in accordance with the HIPAA Security Standards (the security rule), electronic systems with designated record set information should currently be creating access logs with sufficient information to create an access report.³⁴ HHS believes that this new requirement will provide individuals with a “more complete picture” of those who have accessed their information.³⁵ The degree of burden imposed by the new access rights will undoubtedly be the focus of many organizations submitting comments on the proposed rule.

Content of Access Report

The proposed rule specifies that the access report would need to include the following elements: (i) the date of the access; (ii) the time of the access; (iii) the name of the individual, if available, or otherwise the name of the entity who accessed the information; (iv) a description of what information was accessed, if available; and (v) a description of the action by the user, if available.³⁶ A description of a user’s action might use terms such as “create,” “modify,” “access,” or “delete.”³⁷ Unlike an accounting, the access report need not include the address of the user or a description of the purpose of the access.³⁸ Furthermore, the access report is not required to include the ultimate recipient of the electronic PHI, unless the recipient is the natural person or entity with direct access to the electronic PHI.³⁹

HHS notes that the information contained in an access report will be similar to the data that information technology professionals commonly refer to as “audit log data.”⁴⁰ Although electronic designated record set information will often reside on a number of distinct systems with separate access logs, HHS expects covered entities to aggregate that data into a single access report.⁴¹

As noted above with regard to an individual’s option to limit his or her accounting to certain disclosures, the proposed rule would require covered entities to provide individuals with the option to limit the access report to a specific date, time period or person.⁴² HHS believes that this more streamlined report would be mutually beneficial to covered entities and individuals. While not a requirement, the proposed rule also would encourage covered entities to provide individuals with the option to limit the access report to specific organizations.⁴³

³⁴ 76 Fed. Reg. at 31437.

³⁵ 76 Fed. Reg. at 31436.

³⁶ 76 Fed. Reg. at 31437- 38 (to be codified at 45 C.F.R. § 164.528(b)(2)(i)(A)–(E)).

³⁷ 76 Fed. Reg. at 31438.

³⁸ 76 Fed. Reg. at 31438-39.

³⁹ 76 Fed. Reg. at 31439.

⁴⁰ 76 Fed. Reg. at 31436.

⁴¹ 76 Fed. Reg. at 31439.

⁴² 76 Fed. Reg. at 31439 (to be codified at 45 C.F.R. § 164.528(b)(2)(ii)).

⁴³ 76 Fed. Reg. at 31439- 40 (to be codified at 45 C.F.R. § 164.528(b)(2)(ii)).

The access report would also need to be provided in a format that is understandable to the individual and may be provided in a machine-readable or other electronic form and format requested by the individual.⁴⁴

Provision of the Access Report

The proposed rule would impose a 30-day timeline for providing the access report, much like the proposed timeline for the accounting of disclosures discussed above.⁴⁵ This means that within the 30-day period, a covered entity also would need to include the access logs of its business associates that create, receive, maintain, or transmit electronic designated record set information.⁴⁶ While one 30-day extension may be permitted, the covered entity would need to provide the individual with a written statement describing the reason for the delay and the date by which the covered entity will provide the access report.⁴⁷

As with the accounting of disclosures, the proposed rule would not permit a covered entity to charge for providing the first access report to an individual in any 12-month period.⁴⁸ A covered entity may charge a reasonable, cost-based amount for each additional access report that is requested within a 12-month period.⁴⁹

Documentation

Under the proposed rule, covered entities would have the same documentation requirements for access reports as for accountings of disclosures. This means that covered entities would need to retain the necessary documentation to produce access reports for three years.⁵⁰ Copies of the actual access reports, however, would need to be retained for six years.⁵¹

Notice of Privacy Practices

Under the proposed rule, a covered entity would need to provide an individual with a notice of privacy practices that contains a statement of the individual’s right to receive both an accounting of disclosures of PHI and an access report.⁵² Because the access report requirement is new, it would require an amendment to existing privacy notices. HHS notes that such an amendment would constitute a material change to the policy.⁵³

⁴⁴ 76 Fed. Reg. at 31440 (to be codified at 45 C.F.R. § 164.528(b)(2)(iii)).

⁴⁵ 76 Fed. Reg. at 31440 (to be codified at 45 C.F.R. § 164.528(b)(3)(i)).

⁴⁶ 76 Fed. Reg. at 31440.

⁴⁷ 76 Fed. Reg. at 31440 (to be codified at 45 C.F.R. § 164.528(b)(3)(i)(B)(1)–(2)).

⁴⁸ 76 Fed. Reg. at 31440 (to be codified at 45 C.F.R. § 164.528(b)(3)(iii)(A)).

⁴⁹ 76 Fed. Reg. at 31440 (to be codified at 45 C.F.R. § 164.528(b)(3)(iii)(B)).

⁵⁰ 76 Fed. Reg. at 31440 (to be codified at 45 C.F.R. § 164.528(b)(4)(i)).

⁵¹ 76 Fed. Reg. at 31440 (to be codified at 45 C.F.R. § 164.528(b)(4)(ii)(A)–(B)).

⁵² 76 Fed. Reg. at 31441 (to be codified at 45 C.F.R. § 164.520(b)(1)(iv)(E)).

⁵³ *Id.*