



# HEALTH IT LAW & INDUSTRY



VOL. 3, NO. 44

OCTOBER 31, 2011

## OCR's Proposed Revisions to Accounting for Disclosures Standard Produce Strong Opposition From Many Covered Entities



By JENNIFER S. GEETTER, DANIEL F. GOTTLIEB, AND  
BERNADETTE M. BROCCOLO

### Introduction

The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) is reviewing comments submitted by interested parties to OCR's proposed rule (Proposed Rule)<sup>1</sup> to implement a provision<sup>2</sup> of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) that expands the accounting for disclosures standard under the privacy standards (Privacy Standards) adopted under the Health Insurance Portability and Accountability

Act of 1996 (HIPAA). The HITECH Act provision requires health care providers, health plans and other HIPAA covered entities (Covered Entities) to account for disclosures of Protected Health Information<sup>3</sup> (PHI) made through an electronic health record<sup>4</sup> for treatment, payment and health care operations purposes. Based on comments made publicly available by the commenters, the Proposed Rule has engendered vigorous opposition within the health care industry.

The Proposed Rule follows OCR's request for information from interested parties and the public on implementation of the HITECH Act provision on May 3, 2010 (Request For Information).<sup>5</sup> OCR indicates in the preamble to the Proposed Rule that responses to the Request For Information influenced the drafting of the Proposed Rule.

OCR also uses the Proposed Rule as a vehicle to propose other changes to improve the "workability and effectiveness" of the accounting standard.<sup>6</sup> OCR would essentially divide the accounting standard into two distinct requirements. (OCR's proposed changes are summarized in Table 1 at the end of this White Paper.) First, individuals would continue to have a somewhat more limited version of the current right to an accounting of

<sup>1</sup> 76 Fed. Reg. 31426 (proposed May 31, 2011) (to be codified at 42 C.F.R. Part 164).

<sup>2</sup> 42 U.S.C. § 17935(c) (2006).

*The authors are attorneys in the health care practice at McDermott Will & Emery LLP. Geetter can be contacted at jgeetter@mwe.com or (202) 756-8205. Gottlieb can be contacted at dgottlieb@mwe.com or (312) 984-6471. Broccoli is a member of the Advisory Board for BNA's Health IT Law & Industry Report and can be contacted at bbroccoli@mwe.com or (312) 984-6911.*

<sup>3</sup> See 45 C.F.R. § 160.103 (2010) for a definition.

<sup>4</sup> 42 U.S.C. 17291(5).

<sup>5</sup> 75 Fed. Reg. 23214 (May 3, 2010); see also our On the Subject, entitled, "HHS Issues Request for Information on HITECH Act Requirement for Accounting For Disclosures Through an Electronic Health Record."

<sup>6</sup> 76 Fed. Reg. at 31426.

disclosures of PHI, unless an exception applies. This is the pre-HITECH net accounting standard (Current Accounting Standard).

Second, individuals would have a new right to obtain a report (referred to as an Access Report) identifying an employee or other person who has accessed PHI in an electronic Designated Record Set (as defined below) rather than only the right to gain access to what is more conventionally considered an electronic health record—a computerized version of a health care provider’s medical records, unless an exception applies (Access Report Requirement). A Designated Record Set includes any of the following: medical records and billing records of a health care provider; enrollment, payment, claims adjudication or case or medical management record systems of a health plan; and other records used by a Covered Entity to make decisions about individuals.<sup>7</sup> Arguably, tying the Access Report to an electronic Designated Record Set exceeds the HITECH Act requirement that a Covered Entity account for disclosures made through an electronic health record. However, the HITECH Act included an expansive definition of electronic health record that is similar in substance to the HIPAA regulations’ broad definition of a Designated Record Set rather than describing a merely computerized version of a health care provider’s record of clinical services provided to a patient.

The Access Report Requirement is OCR’s proposal to implement the HITECH Act’s expansion of the Current Accounting Standard. The breadth of the Access Report Requirement and the logistics in generating a single report across disparate and varied electronic systems has generated significant concern<sup>8</sup> among Covered Entities and their business associates (Business Associates)<sup>9</sup> that would need to collect and report the access information. OCR acknowledged that the process for meeting the Proposed Rule’s accounting standard and Access Report Requirement is time consuming and expensive but anticipated that the process of generating an Access Report would be automated and would piggyback on existing requirements in the HIPAA security standards (Security Standards) for audit logs. However, various commenters have noted that the Security Standards’ audit log requirements are less prescriptive and instead allow for an approach that is tailored to the resources and technology of the Covered Entity.<sup>10</sup> Thus, there remains a significant difference of opinion regarding the ability of Covered Entities and Business Associates to leverage current systems to comply with the proposed Access Report Requirements.

<sup>7</sup> 45 C.F.R. § 164.501.

<sup>8</sup> See, e.g., American Hospital Association’s model comments to the Proposed Rule at <http://www.aha.org/aha/letter/2011/110720-cl-hitechacctdiscl.docx?group=hospital>.

<sup>9</sup> See 45 C.F.R. § 160.103 for a definition.

<sup>10</sup> See, e.g., American Hospital Association’s model comments to the Proposed Rule at <http://www.aha.org/aha/letter/2011/110720-cl-hitechacctdiscl.docx?group=hospital>.

OCR does not believe that including electronic billing systems and other electronic clinical systems (which maintain Designated Record Sets) beyond conventional electronic health records places an undue burden on Covered Entities and Business Associates because the existing Security Rule requires systems that maintain electronic PHI to include audit log functionality.<sup>11</sup> OCR also stated that it would be difficult for Covered Entities to distinguish what components of a Designated Record Set constitute electronic health records as the “concept of what constitutes an EHR is in a state of flux.”<sup>12</sup>

OCR indicates that the Current Accounting Standard (as amended by the Proposed Rule) and the Access Report Requirements would be “distinct but complementary.”<sup>13</sup> The purpose of the Access Report is to inform individuals about *who* has accessed their electronic Designated Record Set information rather than the *purpose* for such access. The purpose of the Proposed Rule’s accounting standard is to provide more fulsome information on a subset of disclosures thought to be of the greatest interest to individuals. OCR stated that it believed that the two related requirements would provide individuals with information of the greatest interest and import “while placing a reasonable burden on covered entities and business associates.”<sup>14</sup>

OCR proposes that Covered Entities and Business Associates provide individuals with a right to an Access Report beginning January 1, 2013, for electronic Designated Record Set systems acquired after January 1, 2009, and beginning January 1, 2014, for electronic Designated Record Set systems acquired on or before January 1, 2009.<sup>15</sup> Covered Entities would be required to comply with OCR’s changes to the accounting of disclosure requirements 180 days after the effective date of the final rule implementing the changes. Since the effective date of the final rule will be 60 days after publication in the Federal Register, Covered Entities will have 240 days to come into compliance with the changes.

This White Paper includes the following sections:

**Part I:** Current Accounting Standard

**Part II:** Proposed Access Report Requirement

**Part III:** Other Proposed Changes to Accounting Standard

## Part I. Current Accounting Standard

The Current Accounting Standard requires Covered Entities to make available to individuals a list (called an accounting) of electronic, paper or oral “disclosures” of PHI made by the Covered Entity or its Business Associates during the six-year period prior to the request unless one of the exceptions discussed below applies.<sup>16</sup>

<sup>11</sup> 76 Fed. Reg. at 31437. See 45 C.F.R. 64.312(b) for the Security Rule audit control requirement.

<sup>12</sup> 76 Fed. Reg. at 31437.

<sup>13</sup> 76 Fed. Reg. at 31429.

<sup>14</sup> *Id.*

<sup>15</sup> 76 Fed. Reg. at 31429.

<sup>16</sup> 45 C.F.R. § 164.528(a)(1).

To request permission to reuse or share this document, please contact [permissions@bna.com](mailto:permissions@bna.com). In your request, be sure to include the following information: (1) your name, company, mailing address, e-mail and telephone number; (2) name of the document and/or a link to the document PDF; (3) reason for request (what you want to do with the document); and (4) the approximate number of copies to be made or URL address (if posting to a website).

This requirement applies regardless of whether the PHI is maintained in a Designated Record Set.

A disclosure is “the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.”<sup>17</sup> The accounting must include the following information: (1) the date of the disclosure; (2) the name of the recipient; (3) the address of the recipient (if known); (4) a brief description of the information that was disclosed; and (5) a brief description of the reason the information was disclosed or a copy of the original request for the information.<sup>18</sup> A Covered Entity is not required to account for *internal* “use” of PHI by employees or other workforce members under the Current Accounting Standard.

The Current Account Standard does not require a Covered Entity to account for disclosures made under the following conditions: (1) to perform treatment, payment or health care operations functions; (2) to an individual of PHI pertaining to them; (3) incident to a permitted use or disclosure; (4) pursuant to a valid authorization; (5) for the facility’s directory, to persons involved in an individual’s care, or other notification purposes enumerated in the Privacy Standards; (5) in furtherance of national security or intelligence gathering; (6) to correction institutions or law enforcement; (7) as part of a limited data set; and (8) that occurred prior to the compliance date.<sup>19</sup>

## Part II: Proposed Access Report Requirement

### HITECH ACT REQUIREMENTS

The HITECH Act provides that the exception under the Current Accounting Standard for disclosures for treatment, payment and health care operations no longer applies if the disclosure is made “through an electronic health record.”<sup>20</sup> The HITECH Act defines an electronic health record broadly 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.” Given the broad language in the definition, OCR appears to have the authority to require an accounting of disclosures beyond disclosures made through what is commonly understood to be a health care provider’s electronic health record. However, the HITECH Act directs HHS to propose an approach that balances the individual’s need for and interest in information with the burdens on Covered Entities and Business Associates.<sup>21</sup>

<sup>17</sup> 45 C.F.R. § 160.103.

<sup>18</sup> 45 C.F.R. § 164.528(b)(2).

<sup>19</sup> 45 C.F.R. § 164.528(a). In addition, in connection with disclosures made for research purposes pursuant to a waiver or authorization involving 50 or more subjects, the current Privacy Standards permit a Covered Entity to provide to an individual a list of research protocols rather than specific information. The individual therefore receives a list of protocols in which his/her PHI *may* have been used and contact information for those studies rather than confirmed information about the specific studies in which the individual’s PHI was disclosed. 45 C.F.R. § 164.528(b)(4)(i).

<sup>20</sup> 42 U.S.C. 17935(c).

<sup>21</sup> The Act directs HHS to issue regulations that “only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their PHI is being disclosed and takes into account the admin-

## OVERVIEW OF PROPOSED ACCESS REPORT REQUIREMENT

The Proposed Rule would require a Covered Entity to provide individuals with an Access Report identifying the following information for each instance of user access to any Designated Record Set maintained by the Covered Entity or one of its Business Associates during the three-year period preceding the individual’s request for the report (unless an exception applies): (1) the name of the natural person or entity that accessed the PHI; (2) date of the access; and (3) time of the access.<sup>22</sup> OCR proposes that the Access Report include a description of the PHI that was accessed and a description of the user’s action (for example, create, modify, read or print) but only to the extent that the Covered Entity’s or its Business Associates’ existing systems have this capability.<sup>23</sup> OCR did not propose to require the capability where it does currently exist because the burden on Covered Entities of updating their systems or implementing new systems outweighs the benefits to individuals, whom OCR believes are principally concerned with *who* has accessed their information and not *why*.<sup>24</sup> The Access Report records neither the recipient of the disclosed PHI (in the case of a disclosure by a system user to a third party), nor the purpose of the use or disclosure (for example, performing health care operations or making a report to law enforcement).<sup>25</sup>

### ACCESS REPORT MUST INCLUDE USES AND DISCLOSURES

The term “access” is intended to refer to both uses and disclosures through an electronic Designated Record Set. Thus, the Proposed Rule’s Access Report Requirement would go beyond the HITECH Act’s expansion of the Current Accounting Standard and require the Access Report to include information on both disclosures to individuals and organizations outside the Covered Entity *and internal uses* of information by the Covered Entity’s employees and other workforce members. Unlike the Current Accounting Standard, however, the Proposed Rule does not require the Access Report to identify uses or disclosures outside of an electronic Designated Record Set.

OCR cites three reasons for requiring an Access Report to include internal uses of PHI even though the HITECH Act only requires an accounting of disclosures outside the Covered Entity:

- OCR believes that individuals want to learn about both internal uses and external disclosures of their PHI.
- Based on the responses to the Request For Information, OCR believes that many security log systems lack the ca-

istrative burden of accounting for such disclosures. *Id.* For more information on the HITECH Act’s amendments to the HIPAA administrative simplification regulations, see our White Paper entitled, “Economic Stimulus Package: Policy Implications of the Financial Incentives to Promote Health IT and New Privacy and Security Protections” which can be found at [http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object\\_id/ea996ed0-ba3b-480a-988a-135230c441d6.cfm](http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/ea996ed0-ba3b-480a-988a-135230c441d6.cfm).

<sup>22</sup> 76 Fed. Reg. at 31437-38 (to be codified at 45 C.F.R. § 164.528(b)(2)).

<sup>23</sup> 76 Fed. Reg. at 31438 (to be codified at 45 C.F.R. § 164.528(b)(2)(D)-(E)).

<sup>24</sup> *Id.* at 31439.

<sup>25</sup> *Id.*

pability to distinguish between uses and disclosures, and therefore the focus on the encompassing term “access” may relieve Covered Entities and Business Associates from having to modify their systems.

- OCR anticipates that Covered Entities and Business Associates currently have security log systems that can record uses and disclosures because the Security Standards already require audit capabilities. The Security Standards require Covered Entities to implement “hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information”<sup>26</sup> and “procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.”<sup>27</sup> However, the Security Standards’ audit log requirement is less prescriptive than the Proposed Rule’s Access Report Requirement. Instead, the Security Standards allow a Covered Entity significant latitude to determine the security controls that are reasonable and appropriate in the Covered Entity’s information technology environment.<sup>28</sup>

### EXCEPTIONS TO ACCESS REPORT REQUIREMENT

OCR does not believe that the same exceptions available for the Current Accounting Standard are necessary for Access Report Requirement<sup>29</sup> because the Access Report will not be required to include the purpose of the access and will not include the name of the recipient unless the recipient is also the user with direct access to the PHI). For example, the Proposed Rule does not exclude from the Access Report Requirement Standard access to PHI for purposes of making law enforcement disclosures since law enforcement would typically not have direct access to a Designated Record Set. In addition, information meeting the definition of patient safety work<sup>30</sup> product may be omitted from an Access Report.<sup>31</sup>

### FORM AND FORMAT

The Proposed Rule would require that the Covered Entity provide the Access Report in a form and format that can be easily understood by the requesting individual.<sup>32</sup> The Covered Entity must provide the Access Report in a machine readable or other electronic form and format that is specified by the individual if easily producible. In those cases where it is not easily producible, the Covered Entity may provide a hard copy instead.<sup>33</sup> A Covered Entity would be required to provide the Access Report under the same timetable as an accounting and the same fee charging rules would apply.<sup>34</sup>

### REVISION TO NOTICE OF PRIVACY PRACTICES

The Proposed Rule requires Covered Entities to modify their notice of privacy practices to include the

individual’s right to an Access Report.<sup>35</sup> Because this would constitute a “material change” to the notice, the Privacy Standards require that certain steps be taken to notify patients of the change. Covered Entity health care providers with a direct treatment relationship with the patient must make the notice available upon request as of the effective date of the revision and promptly post the notice at any delivery sites with copies for individuals to take with them.<sup>36</sup> Health plans must distribute revised notices within 60 days of the effective date of the revision.<sup>37</sup> OCR notes that health plans may incur significant costs in meeting this requirement and is considering a number of options to take these burdens into account.<sup>38</sup>

### RELATIONSHIP TO EHR CERTIFICATION CRITERIA

The HHS Office of the National Coordinator for Health Information Technology (ONC) adopted final standards, implementation specifications and certification criteria for EHR technology to qualify as certified EHR technology for Stage 1 of the Medicare and Medicaid EHR incentive programs, which became effective August 27, 2010 (Certification Requirements).<sup>39</sup> The Certification Requirements include a standard and certification criterion for the capability to record date, time, patient identification, user identification, and a description of the disclosure for each disclosure that a hospital or professional made for treatment, payment and health care operations.<sup>40</sup> The standard and certification criterion do not require EHR technology to account for internal uses of PHI by a Covered Entity’s workforce. The standard and criterion are intended to implement the accounting standard of the Privacy Standards, but are optional for certification purposes.<sup>41</sup> Accordingly, EHR technology may be certified for Stage 1 of the Medicare and Medicaid EHR Incentive Programs even if it does not facilitate the provision of an Access Report or accounting. OCR indicated that it intends to coordinate with ONC alignment of the Privacy Standards with the EHR certification regulations. For more information on the Certification Requirements, see our White Paper entitled, “Navigating the Government’s Final Rules for Earning Incentive Dollars Through Meaningful Use of E-Health Record Technology” which can be found at [http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object\\_id/ccead80f-e0e4-4078-8027-5dab6fd697b5.cfm](http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/ccead80f-e0e4-4078-8027-5dab6fd697b5.cfm).

### Part III. Other Proposed Changes to Current Accounting Standard

The Proposed Rule would amend the Current Accounting Standard to narrow the accounting to certain

<sup>35</sup> 76 Fed. Reg. at 31441 (to be codified at 45 C.F.R. § 164.520(b)(1)(iv)(E)).

<sup>36</sup> *Id.* (to be codified at 45 C.F.R. § 164.520(c)(2)(iv)).

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

<sup>39</sup> Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Interim Final Rule, 75 Fed. Reg. 2013 (codified at 45 C.F.R. Part 170) (January 13, 2010), available at <http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf>.

<sup>40</sup> 45 C.F.R. § 170.210(e) and 170.302(v).

<sup>41</sup> *Id.*

<sup>26</sup> 45 C.F.R. § 154.312(b).

<sup>27</sup> *Id.* § 164.308(a)(1)(ii)(D).

<sup>28</sup> *Id.* § 164.306(b).

<sup>29</sup> 76 Fed. Reg. at 31439 (to be codified at 45 C.F.R. § 164.528(c)).

<sup>30</sup> Patient safety work product is defined at 42 C.F.R. § 3.20.

<sup>31</sup> 76 Fed. Reg. at 31439.

<sup>32</sup> 76 Fed. Reg. at 31440 (to be codified at 45 C.F.R. § 164.528(b)(2)(E)(iii)).

<sup>33</sup> *Id.* (to be codified at 45 C.F.R. § 164.528(b)(3)(ii)).

<sup>34</sup> *Id.* (to be codified at 45 C.F.R. § 164.528(b)(3)(i)(B)).

disclosures of PHI in an electronic or paper Designated Record Set, exclude additional disclosures from the Current Accounting Requirement and reduce the accounting look-back period to three years. The proposed amendments are discussed below.

## DESIGNATED RECORD SET

The Proposed Rule would no longer require Covered Entities to account for disclosures of PHI not maintained in a Designated Record Set.<sup>42</sup> As a result, Covered Entities would no longer be required to account for records containing PHI that are not used to make clinical, billing or payment decisions about an individual. For example, a hospital would not be required to account for a disclosure of PHI in peer review records that are used to make credentialing and quality improvement decisions instead of clinical and payment decisions.

The right of accounting extends to disclosures to and by Business Associates of PHI maintained in Designated Record Sets.<sup>43</sup> However, since many Business Associates do not maintain Designated Record Sets, many Business Associates would no longer need to account for disclosures of PHI.

## EXCEPTIONS TO ACCOUNTING REQUIREMENT

The Current Accounting Standard lists the categories of disclosures that are excepted from the accounting requirement.<sup>44</sup> The Proposed Rule revises the standard to specify which disclosures of PHI in a Designated Record Set are accountable.<sup>45</sup>

The Proposed Rule preserves the categories of disclosures excepted from the Current Accounting Standard. In addition, the Proposed Rule would exclude the following additional categories of disclosures:

- About victims of abuse, neglect or domestic violence
- For health oversight activities
- For certain research purposes<sup>46</sup>
- Pursuant to waivers of authorization for research
- About decedents to coroners and medical examiners, funeral directors, and for cadaveric organ, eye or tissue donation purposes
- For protective services for the President and enumerated others
- Patient safety work product<sup>47</sup>

However, the Proposed Rule provides that disclosures that would otherwise require an accounting, for example, public health disclosures, that are also required (as opposed to permitted) by law would not be subject to the accounting requirement.<sup>48</sup> Nonetheless, Covered Entities and Business Associates must still make an accounting of disclosures for judicial and administrative proceedings and for law enforcement pur-

poses, even when such disclosures are required by law.<sup>49</sup> The Proposed Rule explains this different approach by noting disclosures for law enforcement and judicial and administrative proceedings “directly implicate an individual’s legal and/or personal interests” and therefore an individual has a need and right to learn of such disclosures.<sup>50</sup>

## RELATIONSHIP TO HITECH BREACH NOTIFICATION REQUIREMENTS

The Breach Notification Standards require Covered Entities to notify individuals of a breach of unsecured PHI. Subject to certain exceptions, a breach is the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the Privacy Standards which poses a significant risk of financial, reputational, or other harm to the individual. The Proposed Rule’s accounting standard would require a Covered Entity to account for a disclosure of PHI that is not permitted by the Privacy Standards even if it does not pose a significant risk of harm to an individual or otherwise meets an exception to the Breach Notification Standards’ breach definition.<sup>51</sup> Therefore, the Proposed Rule would allow individuals to learn about impermissible disclosures that do not require a breach notification letter.

## CONTENT OF ACCOUNTING

The Proposed Rule proposes to maintain the current content of an accounting with minor modifications. First, the accounting would only need to provide an “approximate” date or period of time for each disclosure if the precise date is not known.<sup>52</sup> In all cases, the date must include a month and a year or a description of when the disclosure occurred so that the individual can easily determine the month and year.<sup>53</sup> For multiple disclosures of PHI to the same person/entity for the same purpose, the Proposed Rule would permit a Covered Entity to identify an approximate period of time (for example, January 2011 through June 2011).<sup>54</sup> However, an exact start and end date would no longer be required.

As a general rule, the Proposed Rule would require an accounting to include the name of the recipient of the disclosed information; however, the Proposed Rule would not require the name of the recipient if this would itself represent a disclosure of PHI.<sup>55</sup> For example, if a mail merge error resulted in health plan beneficiaries receiving an explanation of benefits corresponding to the beneficiary next in alphabetic order, the recipient would be entitled to privacy protection as well. Rather, in such cases, the accounting requirements could be met by indicating that the disclosure was to “another patient” or other language that would not compromise an individual’s privacy.

The Current Accounting Standard requires that the accounting include “a brief description of the PHI dis-

<sup>42</sup> 76 Fed. Reg. at 31430 (to be codified at 45 C.F.R. § 164.528(a)(1)(i)).

<sup>43</sup> *Id.*

<sup>44</sup> 45 C.F.R. § 164.528(a)(l).

<sup>45</sup> 76 Fed. Reg. at 31431 (to be codified at 45 C.F.R. § 164.528(a)(1)).

<sup>46</sup> 45 C.F.R. § 164.512(i).

<sup>47</sup> Patient safety work product is defined at 42 C.F.R. § 3.20 (2010).

<sup>48</sup> 76 Fed. Reg. at 31431 (to be codified at 45 C.F.R. § 164.528 (a)(1)(ii)).

<sup>49</sup> *Id.* (to be codified at 45 C.F.R. § 164.528(a)(1)(i)(C)-(D)).

<sup>50</sup> *Id.* at 31434.

<sup>51</sup> *Id.* at 31431 (to be codified at 45 C.F.R. § 164.528 (a)(1)(A)).

<sup>52</sup> *Id.* 31434 (to be codified at 45 C.F.R. § 164.528 (a)(2)(i)(A)(1)).

<sup>53</sup> *Id.*

<sup>54</sup> *Id.* at 31434 (to be codified at 45 C.F.R. § (a)(2)(i)(A)(2)).

<sup>55</sup> *Id.* (to be codified at 45 C.F.R. § 164.528(a)(2)(i)(B)).

closed.”<sup>56</sup> The Proposed Rule would modify this slightly to read “a brief description of the type of PHI disclosed.”<sup>57</sup> Covered Entities would still be permitted to meet this requirement by providing a copy of the written request that triggered the disclosure if it better informs the individual of the purpose of the disclosure.

### ACCOUNTING LOOK-BACK PERIOD

The HITECH Act changes the accounting period from six to three years preceding the request.<sup>58</sup> The Proposed Rule would reduce to three years the time frame for retaining information that is retained solely to make an accounting.<sup>59</sup> The Proposed Rule would still require a Covered Entity to retain for six years a copy of any accounting provided and documentation of the designation of who is responsible for handling accounting requests.<sup>60</sup>

### TIMING OF DELIVERY OF ACCOUNTING

The Proposed Rule includes three modifications to the required timing of delivery of an accounting under the Current Accounting Standard:

<sup>56</sup> *Id.*

<sup>57</sup> 76 Fed. Reg. at 31434 (to be codified at 45 C.F.R. § 164.528(a)(2)(i)(C)). The purpose of this proposed change is to reinforce that “the accounting is only required to provide information about the types of PHI that were the subject of the disclosure” and a “minimum description [that] reasonably informs the individual of the purpose [of the disclosure].” *Id.*

<sup>58</sup> 42 U.S.C. § 17935(c)(1)(B).

<sup>59</sup> 76 Fed. Reg. at 31436 (to be codified at 45 C.F.R. § 164.528(a)(5)).

<sup>60</sup> 45 C.F.R. § 164.530(j)(2).

- A Covered Entity’s response time would be reduced from 60 days to 30 days because OCR believes it should not take longer than 30 days.<sup>61</sup>
- A Covered Entity may obtain a one-time 30-day extension.<sup>62</sup>
- If law enforcement requests a delay in making an accounting in connection with an ongoing law enforcement investigation, the Covered Entity must make a timely account of all other accountable disclosures and then supplement the report with information about the law enforcement disclosure once the law enforcement delay expires.<sup>63</sup>

### FORM AND FORMAT OF ACCOUNTING

The Proposed Rule would require a Covered Entity to provide an accounting in a form and format requested by the individual if it is readily producible. If the requested form or format is not readily producible, the Covered Entity may provide a hard copy or work with the individual to seek to identify another acceptable form and format.<sup>64</sup>

<sup>61</sup> 76 Fed. Reg. 31435 (to be codified at 45 C.F.R. § 164.528(a)(3)(i)).

<sup>62</sup> *Id.* at 31435 (to be codified at 45 C.F.R. § 164.528(a)(3)(i)(B)(2)).

<sup>63</sup> *Id.* at 31435-36 (to be codified at 45 C.F.R. § 164.528(a)(4)).

<sup>64</sup> *Id.* at 31435 (to be codified at 45 C.F.R. § 164.528(a)(3)(ii)).

**Table I: Comparison of Current and Proposed Accounting and Access Report Provisions**

	<b>Current Privacy Standards</b>	<b>Proposed Rule – Accounting of Disclosures</b>	<b>Proposed Rule – Access Report</b>
PHI Covered Accounting or Access Report Requirements	Subject to exceptions set forth below, a Covered Entity must account for disclosures of PHI in electronic, paper or oral PHI, regardless of whether the PHI is maintained in a Designated Record Set	Subject to exceptions set forth below, a Covered Entity must account for disclosures of PHI in electronic, paper or oral PHI maintained in a Designated Record Set	Subject to narrow exception set forth below, a Covered Entity must account for any access to PHI maintained in an Electronic Designated Record Set
Disclosures Only?	Disclosures only	Disclosures only	Uses and disclosures (referred to as “access”)
Look-back period	6 years from the date of the request	3 years from the date of the request	3 years from the date of the request

**Table I: Comparison of Current and Proposed Accounting and Access Report Provisions – Continued**

	<b>Current Privacy Standards</b>	<b>Proposed Rule – Accounting of Disclosures</b>	<b>Proposed Rule – Access Report</b>
Exceptions	<ul style="list-style-type: none"> <li>■ Public health activities, except those involving reports of child abuse or neglect or those required by law</li> <li>■ Judicial and administrative proceedings</li> <li>■ Law enforcement activities</li> <li>■ Aversion of a serious threat to health or safety</li> <li>■ Military and veterans activities</li> <li>■ Department of State’s medical suitability determinations</li> <li>■ Government programs providing public benefits</li> <li>■ Worker’s compensation</li> </ul>	<ul style="list-style-type: none"> <li>■ Current exceptions and the following additional exceptions:</li> <li>■ Disclosures made more than three years prior to the date of the disclosure</li> <li>■ About victims of abuse, neglect or domestic violence</li> <li>■ For health oversight activities</li> <li>■ For certain research purposes</li> <li>■ Pursuant to waivers of authorization for research</li> <li>■ About decedents to coroners and medical examiners, funeral directors, and for cadaveric organ, eye or tissue donation purposes</li> <li>■ For protective services for the President and enumerated others</li> <li>■ Patient safety work product</li> <li>■ Disclosures that required (as opposed to permitted) by law unless the disclosure is required for a judicial or administrative proceeding or law enforcement purposes</li> </ul>	<ul style="list-style-type: none"> <li>■ Narrow exceptions, including:</li> <li>■ PHI which is also patient safety work product</li> </ul>
Content of the Accounting or Access Report	<ul style="list-style-type: none"> <li>■ The date of the disclosure</li> <li>■ The name of the recipient</li> <li>■ the address of the recipient (if known)</li> <li>■ A brief description of the information that was disclosed</li> <li>■ A brief description of the reason the information was disclosed or a copy of the original request for the information</li> </ul>	<p>Maintains the current content of an accounting with minor modifications:</p> <ul style="list-style-type: none"> <li>■ Only need to provide an “approximate” date or period of time for each disclosure if the precise date is not known (must include a month and a year or a description of when the disclosure occurred)</li> <li>■ For multiple disclosures of PHI to the same person/entity for the same purpose, an approximate period of time</li> <li>■ Name of the recipient of the disclosed information unless this would itself represent a disclosure of PHI</li> <li>■ A brief description of the type of PHI disclosed</li> </ul>	<ul style="list-style-type: none"> <li>■ The name of the natural person or entity that accessed the PHI</li> <li>■ Date of the access</li> <li>■ Time of the access</li> </ul>
Form of the Accounting or Access Report	Not specified	<ul style="list-style-type: none"> <li>■ Form and format requested by the individual if it is readily producible</li> <li>■ If the requested form or format is not readily producible, the Covered Entity may provide a hard copy or work with the individual to seek to identify another acceptable form and format</li> </ul>	<ul style="list-style-type: none"> <li>■ Composite of information from all electronic Designated Record Set systems in a single report</li> <li>■ Form and format must be easily understood by the requesting individual</li> <li>■ Machine readable or other electronic form and format that is specified by the individual if easily producible</li> <li>■ In those cases where it is not easily produced in electronic form, the Covered Entity may provide a hard copy instead</li> </ul>

Reproduced [or Adapted] with permission from BNA’s Health IT Law & Industry Report, Vol. 3, No. 44,

(10/31/2011), The Bureau of National Affairs, Inc. (800-372-1033) www.bna.com.