To: Morris D. Linton
From: Cory S. Clements
Date: June 6, 2011
Re: HIPPA Privacy Rule Accounting of Disclosures

I. INTRODUCTION

On May 31, 2011, the Department of Health and Human Services ("Department") issued a Notice of Proposed Rulemaking ("NPRM")[1] as authorized by the HITECH Act of 2009.[2] Primarily, the proposed changes revise 45 C.F.R. §164.528 by dividing it into two separate rights available to individuals: (1) the right to an accounting of disclosures and (2) the right to an access report.

Part II defines important key terms used in this memo. Parts III, IV and V follow the headings of the NPRM. Part III gives an outline of the distinction between an accounting of disclosures and an access report, and includes the Department's intent and purpose for requiring access reports. Part IV provides a condensed, section-by-section explanation of the changes in the NPRM. Part V lists the effective and compliance dates for the proposed rule. Finally, Part VI is a comprehensive list of the Department's specific requests for comment.

II. KEY TERMS

Covered Entity ("CE") means a health plan, a health care clearing house, or a health care provider who transmits covered health care transactions electronically.[3]

Designated Record Set means a group of records maintained by or for a CE that is:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the CE to make decisions about individuals.[4]

Protected Health Information ("PHI") means individually identifiable health information that is transmitted or maintained by electronic media or in any other form or medium.[5]

---

[1] *See* HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act, 76 Fed. Reg. 31426-01 (May 31, 2011) (to be codified at 45 C.F.R. pt. 164).
[2] Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, Div. A, Title XIII, Div. B, Title IV, 123 Stat. 226, 467 (codified as amended in scattered sections of 42 U.S.C.).
[3] *See* 45 C.F.R. § 160.103 (2011).
[4] *See id.* § 164.501.
[5] *Id.* § 160.103.

Disclosure means "the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information."[6]

Electronic Health Record ("EHR") means "an electronic record of health related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."[7]

Machine Readable Data means "digital information stored in a standard format enabling the information to be processed and analyzed by computer" (e.g., the format of MS Word, Excel, text, HTML, or text-based PDF).[8]

III. Overview of the Proposed Rule [9]

Revise 45 C.F.R. § 164.528 by dividing it into two separate rights of individuals:

- Individual's right to an ACCOUNTING OF DISCLOSURES
  - **What:** additional information about the disclosure of designated record set information (hard-copy or electronic) to persons outside the CE and its BAs for certain purposes (e.g., law enforcement, judicial hearings, public health investigations)
  - **Intent:** provide more detailed information ("a full accounting") for certain disclosures most likely to impact the individual
- Individual's right to an ACCESS REPORT
  - **What:** information on who has accessed electronic PHI in a designated record set (includes all electronic access by workforce members and persons outside the CE)
  - **Intent:** allow the individual to learn whether specific persons have accessed that individual's electronic designated record set information
  - **Purpose:** make accounting process more automated and include more comprehensive information (all electronic access—both uses and disclosures)
  - **Content:** date, time, and name of person who accessed electronic designated record set; description of PHI accessed and the user's actions (only to the extent possible); covers a 3-year period; does not distinguish between uses and disclosures.

Revise 45 C.F.R. § 164.520 to inform individuals of their right to an access report and an accounting of certain disclosures.

---

[6] *Id.*
[7] 42 U.S.C.A. § 17921(5) (West 2011).
[8] HIPPA Privacy Rule Accounting of Disclosures under the HITECH Act, 76 Fed. Reg. at 31440.
[9] *Id.* at 31428–29.

IV. SECTION-BY-SECTION OF THE PROPOSED RULE [10]

A. Accounting of Disclosures of Protected Health Information—Section 164.528(a)

1. Standard: right to an accounting of disclosures [11]

The new rule, rather than list the exceptions to the accounting requirement, will explicitly list the types of disclosures that are subject to the accounting. The accounting of disclosures now covers a three-year period, rather than a six-year period. Business Associates ("BAs") are now explicitly included in the accounting requirements. A CE must coordinate with its BAs to collect an accounting of disclosures of PHI in a designated record set and aggregate that information in a complete accounting when requested by an individual. While CEs must continue to account for impermissible disclosures not rising to the level of breach, CEs are not required to account for impermissible disclosures if the CE provided breach notification.

The accounting requirement now focuses on the types of disclosures having a significant legal or personal interest to individuals. These disclosures include the following: for public health activities, 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.

Although particular disclosures of PHI are exempt from the accounting requirement, those disclosures still must be documented in the access report if they are made through direct access to electronic designated record set information. Disclosures exempt from the accounting requirement include the following: reports of child abuse or neglect to a public health authority (or other authority authorized by law);[12] to individuals of PHI about them;[13] incident to a use or disclosure otherwise permitted or required by the Privacy Rule;[14] pursuant to an authorization as provided in § 164.508; for the facility's directory or to persons involved in the individual's care or other notification purposes;[15] for national security or intelligence purposes;[16] to correctional institutions or law enforcement officials;[17] as part of a limited data set;[18] or that occurred prior to the compliance date for the CE. All disclosures through paper records to carry out

---

[10] *Id.* at 31429.
[11] *Id.* at 31429–34.
[12] 45 C.F.R. § 164.512(b)(1)(ii).
[13] *Id.* § 164.502.
[14] *Id.*
[15] *Id.* § 164.510.
[16] *Id.* § 164.512(k)(2).
[17] *Id.* § 164.512(k)(5).
[18] *Id.* § 164.514(e).

treatment, payment and health care operations ("TPO") are also exempt from the accounting requirement.

The new rule also proposes to exclude from the accounting requirement the following types of disclosures: reports of adult victims of abuse, neglect, or domestic violence;[19] for health oversight activities;[20] for research purposes;[21] about decedents to coroners and medical examiners, funeral directors, and for cadaveric organ, eye, or tissue donation purposes;[22] for protective services for the President and others;[23] and most disclosures required by law.

Most disclosures *required* by law do not require accounting. Disclosures merely *authorized* by law, however, do require accounting. And the few disclosures *required* by law that also require accounting include disclosures for judicial and administrative proceedings and for law enforcement purposes.[24]

2. Implementation specification: content of the accounting [25]

First, the accounting must include the date of the disclosure. If the actual date of a disclosure is unknown, an approximate date is sufficient but must include a month and year, or else a description of when the disclosure occurred. For multiple disclosures to the same party for the same purpose, the approximate time period when the disclosures occurred is sufficient.

Second, the accounting must include the name and, if known, address of the entity or person who received the PHI. The exception to providing the name of the person or entity is when including the name in an accounting would itself be a disclosure of PHI. An example of this is when a physician's office sends *patient A*'s appointment reminder to *patient B*—and the office determines that breach notification is unnecessary because the privacy and security of the PHI was not compromised. If *patient A* requests an accounting, this incident would merely need to state that the disclosure was made to "another patient."

Third, the accounting requires a brief description of the "type of" PHI disclosed. The proposed change clarifies that the type of PHI, not the PHI itself, should be described.

Fourth, the accounting must include either a brief "description" of the purpose of the disclosure or a copy of a written request. The proposed rule substitutes the word "description" for the word "statement" to clarify that only a minimum description is required. An example of a minimum description would be "for public health" or "in response to law enforcement request."

---

[19] *Id.* § 164.512(c).
[20] *Id.* § 164.512(d).
[21] *Id.* § 164.512(i).
[22] *Id.* § 164.512(g)–(h).
[23] *Id.* § 164.512(k)(3).
[24] 45 C.F.R. § 164.512(e)–(f).
[25] 76 Fed. Reg. at 31434–35.

Finally, CEs must give individuals the option of requesting a more specific or more limited accounting than the full accounting covering all disclosures in a three-year period. This requirement will help individuals wanting to find out information about specific time periods or about a specific entity.

3. Implementation specification: provision of accounting [26]

The permissible response time to a request for accounting is now 30 days instead of 60 days. CEs must provide an accounting in the form and format requested by the individual if readily producible. CEs may require individuals to submit an accounting request in writing. While a CE may not charge an individual for the first accounting request in a 12-month period, the CE may charge a reasonable and cost-based fee for additional accounting requests in the same 12-month period.

4. Implementation specification: law enforcement and health oversight delay [27]

The proposed rule retains the delay for producing an accounting of disclosures based on an ongoing law enforcement investigation. But there is no longer a delay for health oversight investigations because these investigations are no longer required to be in an accounting.

5. Implementation specification: documentation

"[U]nder the proposed rule, a CE must maintain the documentation necessary to generate an accounting of disclosures for three years, must retain a copy of any accounting that was provided to an individual for six years from the date the accounting was provided, and must retain documentation of the designation of who is responsible for handling accounting requests for six years from the last date the designation was in effect."[28]

B. Right to an Access Report—Section 164.528(b) [29]

1. Standard: right to an access report [30]

An access report includes all uses (not just disclosures) of electronic PHI in any designated record set. Any access to paper records is excluded from the access report. The access report is intended to provide an individual with information about the people who have accessed that individual's PHI. The access report requirement extends to all CEs and BAs maintaining electronic designated record set information, including those that do not have EHR systems. The Department

[26] 76 Fed. Reg. at 31435.
[27] *Id.* at 31435–36.
[28] *Id.* at 31436.
[29] *Id.*
[30] *Id.*at 31436–37.

presupposes that all CEs and BAs maintain access logs as required by the Privacy Rule.

2. Implementation specification: content of the access report [31]

The access log must include the date and time of access, the name of the natural person, if available, or else the name of the entity, a description of what was accessed (if available), and a description of the action by the user (if available), e.g., "create," "modify," "delete." This information must be in a format understandable to the individual, without an external aid.

3. Implementation specification: provision of the access report [32]

CEs will have 30 days, rather than 60 days, to provide the access report, including BA's access logs. If more time is needed, a CE must provide a written statement to the individual including the reason for delay and the date when the CE will provide the access report. CEs are only permitted one extension of time. CEs must provide the access report in a Machine Readable Data format or in a hard copy format, depending on the individual's request. CEs may not charge individuals for a first-time report in any 12-month period but may charge individuals a reasonable, cost-based amount for each additional report within the same 12-month period. CEs may require individuals to submit a request in writing for an access report.

4. Implementation specification: documentation [33]

The same documentation requirements that apply to accountings of disclosures also apply to the access reports. CEs and BAs "must retain the documentation needed to produce an access report (e.g., the necessary access log) for three years . . . , 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 from the last date the designation was in effect."[34]

5. Accounting for disclosures made through electronic Health Information Exchange ("HIE") [35]

Health Information Exchange Organizations ("HIOs") are *not* (yet) required to provide an accounting of disclosures for TPO made through an electronic HIE. But the Department will address this topic again in future rulemaking and will likely change this requirement.

---

[31] *Id.*at 31437–40.
[32] *Id.*at 31440.
[33] *Id.*
[34] *Id.*
[35] *Id.* at 31440–41.

HIOs *are* required to account for disclosures through electronic HIE if the disclosure falls under proposed paragraph (a)(1), such as disclosures for public health. HIOs are required to maintain an access report detailing the date, time and identity of the user accessing the PHI for each access of designated record set information for purposes of electronic HIE.

C. Confidentiality of Patient Safety Work Product [36]

CEs will exclude from accountings of disclosures or access reports any access of information for patient safety activities ("patient safety work product").[37] This exclusion will avoid potential conflicts with the Patient Safety and Quality Improvement Rule.

D. Notice of Privacy Practices—Section 164.520 [38]

CEs are required to update their notice of privacy practices to include a statement regarding an individual's right to receive an access report. Because this is a material change, CEs will have to promptly revise and redistribute their new notice of privacy practices.

Health care providers having a direct treatment relationship with individuals must make the notice available upon request starting on the effective date of the revision. Also, if the provider maintains a physical service delivery site, the provider must promptly post the notice and make it available at the delivery site for individuals to take a copy with them. Health plans are required to distribute notices to current members within 60 days of a material revision.

CEs and BAs do not need to change their notice of privacy practices to reflect the right to receive an access report until the compliance date of either January 1, 2013 or January 1, 2014 (depending on the age of the electronic designated record set systems). The Department is considering relaxing the 60-day notification requirement to allow CEs and BAs to notify individuals covered by their plans through the next annual mailing.

V. Effective and Compliance Dates [39]

The Department proposes separate compliance dates for the new requirements under accountings of disclosures and for the new access reports. For the accounting requirements, CEs and BAs "will have 240 days after publication of the final rule to come into compliance." For the access reports, CEs and BAs will be required to be in compliance on January 1, 2013 for any electronic designated record set systems acquired after January 1, 2009. Otherwise, CEs and BAs will have until January 1, 2014 to comply with the access report requirements.

---

[36] *Id.* at 31441.
[37] *See* 42 C.F.R. § 3.20.
[38] *Id.*
[39] *Id.* at 31441–42.

VI. COMMENT REQUESTED [40]

The Department specifically requested comment on the following key issues:

A(1). Standard: right to an accounting of disclosures

i. The proposal to limit the required accounting to only PHI in a designated record set:
   a. Are there unintended consequences in terms of workability?
   b. Are there unintended consequences to an individual's privacy interests?

ii. Comment on the proposal to account for disclosures over a three-year period.

iii. Comment on the burden it would place on CEs and the benefit it would bestow on individuals to require that the accounting of disclosures include impermissible disclosures that the CE already made known to the individual through breach notification.

iv. Whether there are other categories of public health disclosures that warrant exemption from accounting? Whether carving out exemptions for public health disclosures creates too much confusion among individuals and CEs?

v. Whether certain categories of disclosures, currently subject to accounting, should be exempted from accounting?

vi. Comment on the proposal to exclude categories of disclosure from the accounting requirements.

vii. Comment on the value to individuals of the current accounting of research disclosures.
   a. What may be the most important or useful elements of the current accounting to individuals?
   b. Provide data regarding the following:
      i. the number of protocols that would typically be included in a protocol listing;
      ii. the nature and number of smaller research studies involving the disclosure of PHI of less than 50 people currently requiring a specific accounting;
      iii. the burden on researchers and CEs to provide the requested accountings of disclosures.

viii. Comment on any alternative methods of providing information to individuals about research disclosures.
   a. Comment on the Institute of Medicine's recommendation that CEs provide individuals with a list of all IRB/Privacy Board approved studies.

[40] 76 Fed. Reg. 31426-01 to 31449.

b. Whether a less burdensome type of documentation about the research could be provided to individuals while still retaining sufficient value for individuals?

ix. Whether a shorter 30-day deadline, with a single 30-day extension, will significantly benefit individuals and whether it will place an unreasonable burden on CEs?

A(3). Implementation specification: provision of accounting

i. How much time do CEs require in order to collect the necessary information, including information from BAs, and to generate an accounting of disclosures?

ii. Comment on the burden of providing the accounting in electronic formats as requested by individuals.

B(2). Implementation specification: content of the access report

i. Comment on the burden of providing identifying information about internal systems and the interests of individuals in learning about those internal exchanges.

ii. Are current access logs capable of providing the specific information accessed in designated record set? Is this information important to individuals? What are the potential administrative burdens of the requirement that access reports include a description of the information that was accessed?

iii. What is the potential burden to CEs and benefit to individuals of requiring the access report to include address information indicating where the access occurred?

iv. Is it a good proposal not to require CEs and BAs to include a description of the purpose of access in access reports?

v. Is the Department's assumption correct, that systems within audit logs do not record information about the purpose of the access and ultimate recipient of the information?

vi. What are some ways that these accesses, if excepted from the access report, could be identified and excluded in an automated way?

vii. Comment on the following conclusions:

(1) An individual's right to an access report will require minimal changes to existing information systems;

(2) CEs and BAs that comply with the Security Rule or their BA-agreement already log the information necessary and have the ability to generate an access report;

(3) The aggregation of separate access logs from distinct systems into a single access report, while potentially imposing a significant administrative burden, is

reasonable in light of the individual's interest in learning who has accessed his or her PHI;

(4) The burden of generating access reports is proportionate to the interests of individuals. Because if very few individuals request reports, CEs rarely are burdened to generate reports.

B(3). Implementation specification: provision of the access report

i. Comment on CEs' ability to provide access reports in machine readable or other electronic formats.

Part V. Effective and compliance dates

i. On the compliance date, will CEs be capable of generating access reports covering the preceding three years?

Part VI (B)(4). The impact of adding the right to an access report

i. Comment on the number of anticipated requests for access reports and the burden of tracking access to electronic designated record set information. Will the proposed right to an access report have any unintended effects requiring significant changes to existing systems?

ii. Comment on the burden caused by generating an access report.

iii. Comment on the burden of providing an electronic access report.