FEDERAL REGISTER

Vol. 76 Tuesday,
No. 104 May 31, 2011

Part III

Department of Health and Human Services

45 CFR Part 164
HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 164

RIN 0991–AB62

HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act

AGENCY: Office for Civil Rights, Department of Health and Human Services.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Health and Human Services (HHS or "the Department") is issuing this notice of proposed rulemaking to modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule's standard for accounting of disclosures of protected health information. The purpose of these modifications is, in part, to implement the statutory requirement under the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act" or "the Act") to require covered entities and business associates to account for disclosures of protected health information to carry out treatment, payment, and health care operations if such disclosures are through an electronic health record. Pursuant to both the HITECH Act and its more general authority under HIPAA, the Department proposes to expand the accounting provision to provide individuals with the right to receive an access report indicating who has accessed electronic protected health information in a designated record set. Under its more general authority under HIPAA, the Department also proposes changes to the existing accounting requirements to improve their workability and effectiveness.

DATES: Submit comments on or before August 1, 2011.

ADDRESSES: You may submit comments, identified by RIN 0991–AB62, by any of the following methods (please do not submit duplicate comments):

• *Federal eRulemaking Portal:http://www.regulations.gov*. Follow the instructions for submitting comments. Attachments should be in Microsoft Word, WordPerfect, or Excel; however, we prefer Microsoft Word.

• *Regular, Express, or Overnight Mail:* U.S. Department of Health and Human Services, Office for Civil Rights, Attention: HIPAA Privacy Rule Accounting of Disclosures, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. Please submit one original and two copies.

• *Hand Delivery or Courier:* Office for Civil Rights, Attention: HIPAA Privacy Rule Accounting of Disclosures, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. Please submit one original and two copies. (Because access to the interior of the Hubert H. Humphrey Building is not readily available to persons without Federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. We will post all comments received before the close of the comment period at *http://www.regulations.gov.* Because comments will be made public, they should not include any sensitive personal information, such as a person's social security number; date of birth; driver's license number, state identification number or foreign country equivalent; passport number; financial account number; or credit or debit card number. Comments also should not include any sensitive health information, such as medical records or other individually identifiable health information, or any non-public corporate or trade association information, such as trade secrets or other proprietary information.

FOR FURTHER INFORMATION CONTACT: Andra Wicks, 202–205–2292.

SUPPLEMENTARY INFORMATION:

The discussion below includes a description of the statutory and regulatory background of the proposed rule, a section-by-section description of the proposed modifications, and the impact statement and other required regulatory analyses. We solicit public comment on the proposed rule.

I. Statutory and Regulatory Background

A. The Accounting of Disclosures Under the Current Privacy Rule

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), title II, subtitle F—Administrative Simplification, Pubic Law 104–191, 110 Stat. 2021, provided for the establishment of national standards to protect the privacy and security of personal health information. The Administrative Simplification provisions of HIPAA apply to three types of entities, which are known as "covered entities": health care providers who conduct covered health care transactions electronically, health plans, and health care clearinghouses.

Pursuant to HIPAA, the Department promulgated the Standards for Privacy of Individually Identifiable Health Information, known as the "Privacy Rule," on December 28, 2000 (amended on August 14, 2002). See 65 FR 82462, as amended at 67 FR 53182. The Privacy Rule at 45 CFR 164.528 requires covered entities to make available to an individual upon request an accounting of certain disclosures of the individual's protected health information made during the six years prior to the request. A disclosure is defined at § 160.103 as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information."

For each disclosure, the accounting must include: (1) The date of the disclosure; (2) the name (and address, if known) of the entity or person who received the protected health information; (3) a brief description of the information disclosed; and (4) a brief statement of the purpose of the disclosure (or a copy of the written request for the disclosure). For multiple disclosures to the same person for the same purpose, the accounting is only required to include: (1) For the first disclosure, a full accounting, with the elements described above; (2) the frequency, periodicity, or number of disclosures made during the accounting period; and (3) the date of the last such disclosure made during the accounting period.

Section 164.528(a)(1) provides that an accounting must include all disclosures of protected health information, except for disclosures:

• To carry out treatment, payment and health care operations as provided in § 164.506;

• To individuals of protected health information about them as provided in § 164.502;

• Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;

• 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 as provided in § 164.510;

• For national security or intelligence purposes as provided in § 164.512(k)(2);

• To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);

• As part of a limited data set in accordance with § 164.514(e); or

• That occurred prior to the compliance date for the covered entity.

For disclosures for research in accordance with § 164.512(i) (such as disclosures subject to an Institutional Review Board's waiver of authorization) involving 50 or more individuals, § 164.528(b)(4) permits the covered entity to provide a list of research protocols rather than specific information about each disclosure. Accordingly, an individual who requests an accounting of disclosures may receive a list of research protocols with information about each protocol, including contact information, rather than specific information about disclosures for research.

The current accounting provision applies to disclosures of paper and electronic protected health information, regardless of whether such information is in a designated record set. While the obligation to provide an individual with an accounting of disclosures falls to the covered entity, the accounting must include disclosures to and by its business associates. Business associates are required, as a term of their business associate agreements, to make available the information required for the covered entity's accounting.

B. Changes Required by the HITECH Act

Section 13405(c) of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5), provides that the exemption at § 164.528(a)(1)(i) of the Privacy Rule for disclosures to carry out treatment, payment, and health care operations no longer applies to disclosures "through an electronic health record." Section 13400 of the HITECH Act defines an electronic health record ("EHR") 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." Under section 13405(c), an individual has a right to receive an accounting of such disclosures made during the three years prior to the request. With respect to disclosures by business associates through an EHR to carry out treatment, payment, and health care operations on behalf of the covered entity, section 13405(c) requires the covered entity to provide either an accounting of the business associates' disclosures, or a list and contact information of all business associates (enabling the individual to contact each business associate for an accounting of the business associate's disclosures).

The HITECH Act, at section 13405(c), requires the Secretary to promulgate regulations governing what information is to be collected about these disclosures. The regulations "shall 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 protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures."

Additionally, section 13101 of the HITECH Act, which adds section 3004(b)(1) of the Public Health Service Act, requires the Secretary to adopt an initial set of standards, implementation specifications, and certification criteria for EHR technology. These standards, implementation specifications, and certification criteria are required to address the areas set forth in the newly added section 3002(b)(2)(B) of the Public Health Service Act, including the "[t]echnologies that as a part of a qualified electronic health record allow for an accounting of disclosures made by a [HIPAA covered entity] for purposes of treatment, payment, and health care operations (as such terms are defined for purposes of [the HIPAA regulations]." Section 13405(c) links the modifications to the HIPAA accounting requirements to the above standards, providing that the Secretary issue the accounting regulations within six months of the Secretary's adoption of the EHR accounting standard.

In an interim final rule published on January 13, 2010, the HHS Office of the National Coordinator for Health Information Technology (ONC) adopted a standard and certification criterion to account for disclosures at 45 CFR 170.210(e) and 170.302(v), 75 FR 2014, 2044, 2046. The standard and certification criterion provide that certified EHR technology have the capability to record the date, time, patient identification, user identification, and a description of the disclosure, for disclosures made for treatment, payment, and health care operations. ONC published a final rule on July 28, 2010, which retained this standard but made the certification criterion optional. In the final rule (75 FR 44623), ONC discussed its rationale for retaining the standard for accounting for treatment, payment, and health care operations disclosures and making the related certification criterion optional. Accordingly, EHR technology is not required to have the capability to account for treatment, payment, and health care operations disclosures as a condition of certification for meaningful use Stage 1 under the Medicare and Medicaid EHR incentive payment programs. The Office for Civil Rights will continue to work closely with ONC to ensure that the standards and certification criteria for certified EHR technology align with the HIPAA Privacy Rule accounting of disclosures requirement.

The HITECH Act provides that the effective date of the new accounting requirement for HIPAA covered entities that have acquired an EHR after January 1, 2009, is January 1, 2011, or the date that it acquires an EHR, whichever is later. For covered entities that acquired EHRs prior to January 1, 2009, the effective date is January 1, 2014. The statute authorizes the Secretary to extend both of these compliance deadlines to no later than 2013 and 2016, respectively.

II. Request for Information

On May 3, 2010, HHS published a request for information (RFI) seeking further information on individuals' interests in learning of disclosures, the burdens on covered entities in accounting for disclosures, and the capabilities of current technology. We received approximately 170 comments from numerous organizations representing health plans, health care providers, privacy advocates, and other non-covered entities. These comments are summarized below and were considered when drafting this proposed rule.

The first question in the RFI asked about the potential benefits to individuals from receiving an accounting of disclosures, particularly an accounting that included disclosures for treatment, payment, and health care operations. Approximately 10 respondents representing both consumers and covered entities endorsed the benefits of such an accounting in order to foster transparency and patient trust, as well as to discourage inappropriate behavior. Commenters pointed out that the use of audit trails and the right to an accounting of disclosures improves the detection of breaches and assists with the identification of weaknesses in privacy and security practices. Roughly 10 commenters representing covered entities agreed generally that there are potential benefits to transparency, but questioned whether general accountings would provide the type of information that individuals usually seek. The majority of comments, contributed mostly by covered entities, indicated that providing an accounting of

treatment, payment, and health care operations disclosures would provide little to no benefit to individuals (over 80 respondents), while incurring substantial administrative, staffing and monetary burdens (over 120 respondents).

The second and third RFI questions inquired about individuals' awareness of their right to receive an accounting of disclosures, how covered entities ensure individuals are aware of their accounting right, and the number of accounting requests that covered entities have received. Most covered entities responded that individuals are aware of their accounting right from the notices of privacy practices covered entities provide to individuals. The responses indicated that almost 30 covered entity respondents have received no requests for an accounting of disclosures and more than 90 covered entity respondents have received less than 20 requests since the Privacy Rule's 2003 compliance date.

The fourth RFI question asked about individual use of and satisfaction with the information received in accountings of disclosures. Some covered entities reported receiving accounting requests that were prompted by concerns over a specific situation or person that may have accessed their records. Some covered entities also reported individuals withdrawing their requests for an accounting once they realized that inappropriate uses of protected health information (such as inappropriate access by a member of the workforce) would not be included in the accounting. Most covered entities that have received accounting requests were not aware of how the information was used by individuals or if it was useful to them. Consumer advocates were divided on this topic; one indicated that accountings of disclosures have been useful to individuals, and one related that the accountings have likely not been useful to individuals since the reports have lacked information about the treatment, payment and healthcare operations disclosures.

The fifth question in the RFI asked whether an accounting for treatment, payment, and health care operations disclosures should include the following elements and, if so, why: to whom a disclosure was made, and the reason or purpose for the disclosure. This question also asked about the specificity needed regarding the purpose of a disclosure, and to what extent individuals are familiar with activities that may constitute "health care operations." Regarding the recipient of the disclosure, approximately 60% of the comments, representing covered entities and industry, indicated that recipient information should not be included in an accounting of disclosures. In a few cases, concerns about employee privacy, security, and safety were cited as a reason not to include recipient information. On the other hand, almost 40% of commenters, representing consumers, covered entities and industry, felt that information about the recipient would be vital in addressing individuals' concerns regarding inappropriate receipt of their health information.

Over 60% of the commenters, representing covered entities and industry, indicated that the purpose of the disclosure should not be included due to the minimal benefit this information would provide to individuals and the significant difficulty in capturing this information. Since most current systems do not automatically capture the purpose of a disclosure, new actions would be required, resulting in a disruption of provider workflow. In contrast, almost 20% of commenters, representing consumers and covered entities, indicated that an accounting of disclosures would be useless to individuals without a description of the purpose of each disclosure. Almost one third of comments on this issue supported the use of general categories if a description of the purpose of a disclosure is required. Most respondents felt that individuals do not have a good understanding of what may constitute "health care operations."

Question six of the RFI asked about the capabilities of current EHR systems. Almost all comments received on this topic indicated that current EHR systems are unable to distinguish between a "use" and a "disclosure," are decentralized, and cannot generate accountings of disclosures reports automatically, requiring manual entry to assemble a report for each requested accounting. The comments reflected a variety of audit log experiences, representative of the wide range of systems used for various functions in the health care system. According to the comments, most current audit logs retain at least the name or other identification of the individual who accessed the record, the name or other identification of the record that was accessed, the date, the time, and the area, module, or screen of the EHR that was accessed. Comments generally indicated that maintaining current audit logs for three years would incur minimal additional burden; however, increasing the information retained to include additional information about treatment, payment, and health care operations disclosures would create additional storage space burden.

The seventh RFI question asked about the feasibility of the HITECH Act compliance timelines for the new accounting requirements. The HITECH Act provides that a covered entity that has acquired an EHR after January 1, 2009, must comply with the new accounting requirement by January 1, 2011, unless the Department extends this compliance deadline to no later than 2013. Almost all comments received on this topic indicated that the January 1, 2011, deadline would be impossible to meet. Estimates of the time needed to develop and implement the new accounting feature and subsequently install updated systems varied, however many comments indicated needing at least two years past the 2011 date for compliance. Fewer than 10 early adopters of EHRs (acquired before January 1, 2009) responded, generally indicating that they would also need longer than the 2014 date for compliance, and that the timing would be dependent on vendors developing appropriate systems.

Question eight requested input on the feasibility of an EHR module that is exclusively dedicated to accounting for disclosures. Almost 90% of the comments received on this topic indicated that a separate module to produce accounting of disclosures reports would not be an ideal solution due to the significant time and expense needed to develop such a module for limited benefit, given the low number of accounting requests received to date. Comments also indicated a potential for this effort to detract from meaningful use requirements.

The final question of the RFI requested any other information that would be helpful to the Department regarding accounting for disclosures through an EHR to carry out treatment, payment, and health care operations. A large percentage of the comments expressed concerns with the burdens that this new accounting of disclosures requirement would create. These comments cited increased health care costs, reduced patient care time resulting from disruptions in provider workflow, and a potential chilling effect on the adoption of EHR systems, particularly for small providers. In addition, we received suggestions and requests for clarification on the scope of EHRs, disclosures, and disclosures through an EHR.

III. Overview of Proposed Rule

We are proposing to revise § 164.528 of the Privacy Rule by dividing it into two separate rights for individuals:

paragraph (a) would set forth an individual's right to an accounting of disclosures and paragraph (b) would set forth an individual's right to an access report (which would include electronic access by both workforce members and persons outside the covered entity). Our revisions to the right to an accounting of disclosures are based on our general authority under HIPAA and are intended to improve the workability and effectiveness of the provision. The right to an access report is based in part on the requirement of section 13405(c) of the HITECH Act to provide individuals with information about disclosures through an EHR for treatment, payment, and health care operations. This right to an access report is also based in part on our general authority under HIPAA, in order to ensure that individuals are receiving the information that is of most interest.

These two rights, to an accounting of disclosures and to an access report, would be distinct but complementary. The right to an access report would provide information on who has accessed electronic protected health information in a designated record set (including access for purposes of treatment, payment, and health care operations), while the right to an accounting would provide additional information about the disclosure of designated record set information (whether hard-copy or electronic) to persons outside the covered entity and its business associates for certain purposes (*e.g.,* law enforcement, judicial hearings, public health investigations). The intent of the access report is to allow individuals to learn if specific persons have accessed their electronic designated record set information (it will not provide information about the purposes of the person's access). In contrast, the intent of the accounting of disclosures is to provide more detailed information (a "full accounting") for certain disclosures that are most likely to impact the individual.

We believe that these changes to the accounting requirements will provide information of value to individuals while placing a reasonable burden on covered entities and business associates. The process of creating a full accounting of disclosures is generally a manual, expensive, and time consuming process for covered entities and business associates. In contrast, we believe that the process of creating an access report will be a more automated process that provides valuable information to individuals with less burden to covered entities and business associates. By limiting the access report to electronic access, the report will include information that a covered entity is already required to collect under the Security Rule. Under §§ 164.308(a)(1)(ii)(D) and 164.312(b) of the HIPAA Security Rule, a covered entity is required to record and examine activity in information systems and to regularly review records of such activity. Accordingly, our proposal attempts to shift the accounting provision from a manual process that generates limited information to a more automated process that produces more comprehensive information (since it includes all access to electronic designated record set information, whether such access qualifies as a use or disclosure). We believe that these two rights, in conjunction, would provide individuals with greater transparency regarding the use and disclosure of their information than under the current rule.

The right to an accounting of disclosures would encompass disclosures of both hard copy and electronic protected health information that is maintained in a designated record set. It would cover a three-year period, and would require a covered entity and its business associates to account for the disclosures of protected health information that we believe are of most interest to individuals. The right to an access report would only apply to protected health information about an individual that is maintained in an electronic designated record set. Our proposed rule would provide an individual with a right to obtain a copy of this information in the form of an "access report." It would cover a three-year period, and would provide the individual with information about who has accessed the individual's electronic protected health information held by a covered entity or business associate. It would not distinguish between "uses" and "disclosures," and thus, would apply when any person accesses an electronic designated record set, whether that person is a member of the workforce or a person outside the covered entity. We propose to require that the access report identify the date, time, and name of the person (or name of the entity if the person's name is unavailable) who accessed the information (we also propose to require the inclusion of a description of the protected health information that was accessed and the user's action, but only to the extent that such information is available).

With respect to the right to an accounting of disclosures and the right to an access report, covered entities would be required to include the applicable uses and disclosures of their business associates. Because these rights are limited to protected health information maintained in a designated record set, we believe that some business associates will not be affected by these requirements because they do not have designated record set information.

We are proposing a revision to the requirements for notices of privacy practices at § 164.520 in order to inform individuals of their right to receive an access report, in addition to an accounting of certain disclosures.

We are proposing that covered entities (including small health plans) and business associates comply with the modifications to the accounting of disclosures requirement beginning 180 days after the effective date of the final regulation (240 days after publication). We are proposing 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 as of January 1, 2009.

IV. Section-by-Section Description of Proposed Rule

The following describes the provisions of the proposed rule section by section. Those interested in commenting on the proposed rule can assist the Department by preceding discussion of any particular provision or topic with a citation to the section of the proposed rule being discussed. While we request comment on several specific questions, we welcome comments on any aspects of the proposed rule.

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

We are proposing the following modifications to the existing accounting of disclosures requirements to improve the workability of the requirements and to better focus the requirements on providing the individual with information about those disclosures that are most likely to impact the individual's legal and personal interests, while taking into account the administrative burdens on covered entities and business associates.

1. Standard: Right to an Accounting of Disclosures

Paragraph (a)(1)(i) of the proposed rule would maintain the general standard that an individual has a right to receive an accounting of disclosures by a covered entity or business associate, but would include a number of changes to this right. Specifically, we

propose to change the scope of information subject to the accounting to the information about an individual in a designated record set, to explicitly include business associates in the language of the standard, to change the accounting period from six years to three years, and to list the types of disclosures that are subject to the accounting (rather than listing the types of disclosures that are exempt from the accounting).

Currently, an individual has a right under § 164.528 to an accounting of certain disclosures of protected health information about the individual, regardless of where such information is located. We are proposing to limit the accounting provision to protected health information about the individual in a designated record set. Designated record sets include the medical and health care payment records maintained by or for a covered entity, and other records used by or for the covered entity to make decisions about individuals. See the definition of "designated record set" at § 164.501.

This proposed change would better align the accounting provision at § 164.528 with the individual's rights to access and amend protected health information at §§ 164.524 and 164.526, which are both limited to protected health information about an individual in a designated record set. We believe that this information, which forms the basis for covered entities' health care and payment decisions about the individual, generally represents the protected health information that is of most interest to the individual.

Covered entities should already have documentation of which systems qualify as designated record sets. Currently, § 164.524(e)(1) provides that "[a] covered entity must document the following and retain the documentation as required by § 164.530(j): (1) [t]he designated record sets that are subject to access by individuals; * * *" Covered entities and business associates are likely able to track those disclosures of protected health information within defined and established record sets and systems more easily.

An example of protected health information that may fall outside the designated record set is a hospital's peer review files. If these files are only used to improve patient care at the hospital, and not to make decisions about individuals, then they are not part of the hospital's designated record set. Another example of protected health information that is outside the designated record set are transcripts of customer calls that are used only for purposes of customer service review, rather than to make decisions about the individual.

Note that protected health information outside the designated record set would remain fully protected by the Privacy Rule and, with respect to electronic protected health information, the Security Rule. Further, the Breach Notification Rule continues to apply to all protected health information in any form and regardless of where such information exists at a covered entity or business associates. Thus, individuals would still be informed of breaches of unsecured protected health information even if such information resides outside of a designated record set.

We request comment on our proposal to limit the accounting requirement to protected health information in a designated record set and whether there are unintended consequences with doing so either in terms of workability or the privacy interests of the individual.

We include a direct reference to business associates in the standard to make clear that the covered entity must include accounting information for all disclosures by the covered entity's business associates that create, receive, maintain, or transmit designated record set information. Under the current Privacy Rule, a covered entity is required at § 164.504(e)(2)(ii)(G) to include in its business associate agreements the requirement that the business associate will "make available the information required to provide an accounting of disclosures in accordance with § 164.528." Section 164.528(b)(1) currently provides that the accounting must include "disclosures to or by business associates of the covered entity" without regard to whether such information is maintained within a designated record set. To align with our proposal to apply the accounting requirements only to information within a designated record set, we in turn limit the information held by business associates that is subject to the accounting to information within a designated record set. For example, if a business associate is a third party administrator and maintains a copy of an individual's billing information, the covered entity must coordinate with the business associate to provide an accounting of the disclosures of this information. Similarly, we propose that if a business associate maintains a copy of an individual's medical record, then the covered entity would be required to account for the business associate's disclosure of this information. In contrast, a covered entity would not be required to account for a business associate's disclosure of information outside of a designated record set. As stated above, we believe that this represents the information that is of most interest to individuals, since it is the information that covered entities use to make health care and payment decisions about the individual.

We propose that covered entities and business associates must generally account for disclosures over a three-year period. The current accounting provision requires covered entities and business associates to account for disclosures for the six-year period prior to the request. Section 13405(c)(1)(B) of the HITECH Act, however, states that an individual has a right to receive an accounting of treatment, payment, and health care operations disclosures through an EHR for the three-year period prior to the request. We believe that it is appropriate to maintain a consistent accounting time period for all types of disclosures. Accordingly, our proposal aligns the accounting period for all types of disclosures with the three-year period set forth in section 13405(c)(1)(B) of the HITECH Act. Additionally, based on our experience to date, we believe that individuals who request an accounting of disclosures are generally interested in learning of more recent disclosures (*e.g.,* an individual is seeking information on why she has recently begun to receive information related to her health condition from a third party). Therefore, we do not believe that it will be a significant detriment to individuals to reduce the accounting period from six years to three years. In contrast, we believe it is a significant burden on covered entities and business associates to maintain information on six years of disclosures, rather than three years. We request comment on this issue and if there are specific concerns regarding the need for accounting of disclosures beyond three years.

Paragraph (a)(1)(i) also would address which disclosures are subject to the accounting requirement. We propose to explicitly list the types of disclosures that are subject to the accounting requirement. In contrast, under the current Privacy Rule, § 164.528 provides that disclosures are generally subject to the accounting requirement, but then lists a series of exceptions. We believe that by explicitly listing the exceptions, but not the types of disclosures that are subject to the accounting requirement, the current regulatory language may make it difficult to easily and readily understand the types of disclosures that are subject to the accounting requirement. Thus, our proposed rule takes the opposite approach and explicitly lists the types of disclosures

that are subject to the accounting requirement.

We propose that covered entities will continue to be required to account for disclosures that are impermissible under the Privacy Rule. While individuals will learn of most impermissible disclosures through the Breach Notification Rule at § 164.404, we expect that some individuals will be interested in learning of impermissible disclosures that did not rise to the level of a breach (*e.g.,* because the disclosure did not compromise the security or privacy of the protected health information). This ensures that covered entities and business associates maintain full transparency with respect to any impermissible disclosures by allowing a means (either through receipt of a breach notice or by requesting an accounting) for individuals to learn of all ways in which their designated record set information has been disclosed in a manner not permitted by the Privacy Rule.

We propose to exempt from the accounting requirement impermissible disclosures in which the covered entity (directly or through a business associate) has provided breach notice. We do not believe it is necessary to require the covered entity or its business associates to account for such disclosures since the covered entity has already made the individual aware of the impermissible disclosure through the notification letter required by the Breach Notification Rule. The breach notification requirement serves the same purpose as the accounting requirement, but it is much more rigorous in that it is an affirmative duty on the covered entity to notify the individual of an impermissible disclosure in a more timely and detailed manner than the accounting for disclosures. Nonetheless, covered entities are free to also include in the accounting disclosures for which breach notification has already been provided to the individual if they choose to do so. We request comment on the burdens on covered entities and benefits to individuals associated with also receiving an accounting of disclosures that includes information provided in accordance with the breach notification requirement.

We also propose to continue to include in the accounting requirement 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. We believe that these are the types of disclosures for which individuals are more likely to have a significant legal or personal interest.

We have proposed to continue to include disclosures for public health purposes because, although some public health disclosures are population-based and may have limited impact on individuals, other public health disclosures, such as those related to targeted public health investigations, may be very specific to an individual and could have significant consequences to the individual. As discussed below, if a public health disclosure is also required by law, it would not be subject to the proposed accounting requirement. For example, if a disclosure to a public health authority regarding a communicable disease is required by law, the covered entity would not need to account for the disclosure. In contrast, if a disclosure regarding an individual's communicable disease is authorized, but not required, by law (meaning that it is at the discretion of the covered entity), then the covered entity would be required to account for the disclosure.

Within public health disclosures, however, we are proposing to exempt from the accounting reports of child abuse or neglect to a public health authority or other appropriate government authority authorized by law to receive such reports, as permitted under § 164.512(b)(1)(ii). Since the initial compliance date of the Privacy Rule, a number of entities have raised concerns about the potential harm a covered entity or the members of its workforce may suffer as a result of having to account to a parent or guardian for its reporting to authorities of suspected child abuse or neglect. While the current Privacy Rule at § 164.502(g)(5)(i)(B) provides that a covered entity may elect not to treat a person as an individual's personal representative when the covered entity reasonably believes that doing so could endanger the individual, a covered entity does not have the same discretion when it believes its actions could instead endanger the reporter. Thus, we believe it prudent to exempt such disclosures from the accounting requirement. Further, it is our understanding that the reporting of suspected child abuse or neglect is generally mandated by law and thus, would nonetheless be exempt from the accounting under our proposal (described below) to exempt from the accounting most disclosures that are required by law.

With respect to the remainder of public health disclosures (*i.e.,* public health disclosures other than those related to reports of child abuse or neglect), we request comment on whether there are other categories of public health disclosures that warrant an exception because such disclosures may be of limited interest to individuals and/or because accounting for such disclosures may adversely affect certain population-based public health activities, such as active surveillance programs. We also request comment on whether the complexity of carving out such public health disclosures would lead to too much confusion among individuals and covered entities.

We expect that individuals may have a significant interest in learning of disclosures for judicial and administrative proceedings, law enforcement, and to avert a serious threat to health or safety because such disclosures may significantly impact individuals' legal interests. We thus propose to continue to require that covered entities account for such disclosures.

We propose to continue to require covered entities and business associates to account for disclosures for military and veterans activities under § 164.512(k)(1) and for purposes of the Department of State's medical suitability determinations under § 164.512(k)(4) because such disclosures may have significant employment and benefits consequences to the individual, such as a determination that an individual is not medically able to perform an assignment or mission or not eligible for certain veteran's benefits. In addition, we propose to continue to apply the accounting requirements to disclosures to government programs providing public benefits under § 164.512(k)(6) and for workers' compensation purposes under § 164.512(l) because such disclosures may adversely affect an individual's claim or benefits.

As previously stated, the proposed rule explicitly lists the types of disclosures that are subject to the accounting requirement, rather than the previous approach of listing the types of disclosures for which an accounting was not required. Despite this change in regulatory approach, the following disclosures continue to be excluded from the accounting requirement: (i) To individuals of protected health information about them as provided in § 164.502; (ii) incident to a use or disclosure otherwise permitted or required by the Privacy Rule, as provided in § 164.502; (iii) pursuant to an authorization as provided in

§ 164.508; (iv) for the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510; (v) for national security or intelligence purposes as provided in § 164.512(k)(2); (vi) to correctional institutions or law enforcement officials as provided in § 164.512(k)(5); (vii) as part of a limited data set in accordance with § 164.514(e); or (viii) that occurred prior to the compliance date for the covered entity. How these exceptions are treated for purposes of the access report is discussed below. Disclosures to carry out treatment, payment and health care operations as provided in § 164.506 would continue to be exempt for paper records. However, in accordance with section 13405(c) of the HITECH Act, an individual would be able to obtain information (such as the name of the person accessing the information) for all access to electronic protected health information stored in a designated record set for purposes of treatment, payment and health care operations.

We also request comment on whether the Department should exempt from the accounting requirements certain categories of disclosures that are currently subject to the accounting. In particular, for the reasons discussed below, we are proposing to exclude disclosures about victims of abuse, neglect, or domestic violence under § 164.512(c); disclosures for health oversight activities under § 164.512(d); disclosures for research purposes under § 164.512(i);[1] disclosures about decedents to coroners and medical examiners, funeral directors, and for cadaveric organ, eye, or tissue donation purposes under § 164.512(g) and (h); disclosures for protective services for the President and others under § 164.512(k)(3); and most disclosures that are required by law (including disclosures to the Secretary to enforce the HIPAA Administrative Simplification Rules). Note, however, to the extent such disclosures are made through direct access to electronic designated record set information, such disclosures will be recorded and available to the individual in an access report under proposed § 164.528(b). We request comment on our proposal to exclude these categories from the accounting of disclosures requirements, including comment on the rationales expressed below, and will revisit these exclusions in drafting the final rule based on the public comment we receive.

First, we are proposing to exclude from the accounting requirement disclosures related to reports of adult abuse, neglect, or domestic violence under § 164.512(c). As with the proposal to exclude disclosures for child abuse reporting, we have concerns that accounting for such disclosures could endanger the reporter of the abuse. Further, the Privacy Rule at § 164.512(c)(2) requires the covered entity to promptly inform the individual that an abuse or domestic violence report has been or will be made to the proper authorities unless doing so may endanger the individual. Thus, in most cases, the individual will be affirmatively notified of such disclosures by the covered entity, which obviates the need for the disclosures to be included in an accounting.

In this proposed rule, we are also considering removing from the accounting requirement disclosures for research under § 164.512(i), which includes research where an Institutional Review Board (IRB) or Privacy Board has waived the requirement for individual authorization because, among other reasons, it determined that the study poses no more than a minimal risk to the privacy of individuals and the waiver is needed to conduct the research.[2] Because such research may involve thousands of medical records and the burden to account for each disclosure may have a chilling effect on important areas of study, the current Privacy Rule includes a simplified accounting requirement for larger studies. In particular, the Privacy Rule allows a covered entity to provide individuals with a protocol listing describing the research protocols for which the individual's protected health information may have been disclosed, rather than an individualized accounting of each actual disclosure, for studies involving 50 or more individuals. The protocol listing must include the name of the protocol or other research activity; a plain language description of the research; a brief description of the types of protected health information that were disclosed; the date or period of time during which such disclosures occurred or may have occurred; contact information for the researcher and research sponsor; and a statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or research activity. If it is reasonably likely that the protected health information of the individual was disclosed for a particular research protocol or activity, the Privacy Rule requires that the covered entity assist in contacting the researcher and research sponsor, if requested by the individual. See § 164.528(b)(4)(ii).

Therefore, under the current rule, an individual that requests an accounting of disclosures will receive a specific accounting of certain disclosures (for example, disclosures for research studies involving less than 50 individuals) and a potentially large protocol listing of studies that may or may not include the individual's protected health information. The individual would not be notified of certain disclosures of protected health information for research (such as research in which the individual specifically authorized release of protected health information). In this proposed rule, we are considering whether to exempt covered entities from having to provide an accounting of disclosures for research, including through a protocol listing. Rather, the individual would continue to receive notice through the notice of privacy practices that protected health information may be used or disclosed for research, and the covered entity would only be able to disclose the individual's protected health information for research under limited circumstances (such as based on the individual's authorization or an IRB/Privacy Board finding that the research poses no more than a minimal risk to the individual's privacy).

The Department is considering excluding research disclosures from the accounting requirements because, even though the Privacy Rule includes this simplified accounting option for research disclosures to large studies, the Department continues to hear concerns from the research community regarding the administrative burden of the accounting requirements and the potentially resulting chilling effect the requirements have on human subjects research. For example, the Secretary's Advisory Committee for Human Research Protections (SACHRP) in its September 2004 letter to the Secretary recommended that the Department exempt research disclosures from the accounting requirements altogether. SACHRP indicated that a research protocol listing may be very extensive at

[1] Disclosures of limited data sets for research purposes under § 164.514(e) and disclosures for research purposes pursuant to an individual's authorization under § 164.508 are currently exempt from the accounting requirements and would not be impacted by this proposal.

[2] Section 164.512(i) also permits uses and disclosures for research without an individual's authorization where access to protected health information is sought solely to review the information as necessary to prepare a research protocol or for similar purposes and no protected health information is to be removed from the covered entity by the researcher in the course of the review or where access is being sought solely for research on the protected health information of decedents.

larger institutions and the requirement for a covered entity to assist individuals in contacting the researchers and research sponsors places an unreasonable burden on covered entities. SACHRP further indicated that, since the accounting requirements apply only to research "disclosures" and not "uses," whether access by researchers within institutions to protected health information must be accounted for depends entirely on whether the researchers are workforce members (uses) or physicians with staff privileges (disclosures), which is an "artificial" distinction. See Appendix A to SACHRP's September 27, 2004 letter to the Secretary, available at *http://www.hhs.gov/ohrp/sachrp/appendixa.html.*

Similarly, in a report on ways to enhance privacy and improve health through research, the Institute of Medicine (IOM) concluded that the Privacy Rule's current accounting provision for research disclosures places a heavy administrative burden on health systems and health services research but achieves little in terms of protecting privacy. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research,* Institute of Medicine of the National Academies p. 51 (2009) (available at *http://www.iom.edu*). The IOM report recommended that the Department revise the Privacy Rule to exempt disclosures made for research from the Privacy Rule's accounting requirement. As an alternative, the IOM suggested that all institutions should maintain a list, accessible to the public, of all studies approved by an IRB/Privacy Board.

While acknowledging these concerns, the Department notes that it does not have sufficient information regarding the actual burden, as well as the utility, of providing the current accounting of research disclosures to individuals (*i.e.,* a specific accounting of disclosures for research studies where the disclosures involved less than 50 individuals and a protocol listing of studies where the disclosures involved 50 or more individuals). We thus solicit public comment on the value of the current accounting for research disclosures to individuals who have used or might in the future request such an accounting, including comments on what may be the most important/useful elements of the current accounting to individuals. We also ask covered entities to provide data regarding the number of protocols that would typically be included in a protocol listing, the nature and number of smaller research studies that involve the disclosure by the covered entity of protected health information about less than 50 individuals and for which a specific accounting is currently required, and the burdens on researchers and covered entities to provide the requested accountings of disclosures. Further, we seek public comment on alternative ways that we could provide the individual with information about the covered entity's research disclosures, such as the IOM's recommendation for a list of all IRB/Privacy Board approved studies, or whether other types of documentation about the research could be provided to the individual in a manner that is potentially less burdensome on covered entities but still sufficiently valuable to individuals. We will assess how to best provide information regarding research disclosures to individuals based on these comments.

We note that, as mentioned above, under proposed § 164.528(b), an individual would still be able to request an access report from the covered entity, which would include access for research purposes to electronic designated record set information by workforce members and others, such as physicians with staff privileges (although such electronic access would not be labeled as research).

We also propose to not include disclosures for health oversight activities under § 164.512(d). Such disclosures primarily are population-based or event triggered and thus relate to the covered entity, rather than the individual (if an investigation is focused on the individual rather than the covered entity, then the Privacy Rule at § 164.512(d)(2) generally treats the investigation as for law enforcement rather than health oversight, which means that the disclosure would be subject to the proposed accounting provision). Such disclosures are also often routine, to a government agency, and required by law. For these reasons, we do not believe the potential burden on a covered entity or business associate to account for what may be voluminous disclosures of records is balanced by what is likely not a strong interest on the part of individuals to learn of such disclosures. We request comment on these assumptions.

In addition, we are proposing to not include disclosures about decedents to coroners, medical examiners, and funeral directors under § 164.512(g) because we believe that such types of disclosures are relatively routine, expected, and do not raise significant privacy concerns. Similarly, we propose to exclude disclosures about decedents for cadaveric organ, eye, or tissue donation purposes under § 164.512(h). This limited provision permits a covered entity to disclose protected health information about a decedent in cases where there was no prior HIPAA authorization to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation. The provision is intended to avoid putting covered entities in the position of having to request consent from grieving families with respect to donation of organs of a deceased loved one before a determination has been made that donation would be medically suitable. Given the circumstances and limited nature of the disclosure, and because we anticipate that families will be involved in the decision process with respect to the donation, we propose to exclude these disclosures from the accounting. We request comment on this proposal.

We are proposing to exclude most disclosures that are required by law because these disclosures are often population based rather than related to a specific individual, because they often reflect a determination by a state legislature or other government body rather than a discretionary decision of a covered entity or business associate, and because we believe it is reasonable to assume that individuals are aware that their health information will be disclosed where mandated by law. Further, individuals are generally informed that a covered entity may disclose an individual's protected health information when required to do so by other law through a covered entity's notice of privacy practices. Based on comments received, we have been informed that accounting for these nondiscretionary disclosures represents a significant administrative burden on covered entities. Thus, we propose that disclosures made under § 164.512(a)(1) of the Privacy Rule need not be included in an accounting in order to lessen this administrative burden.

In addition, in paragraph (a)(1)(ii), we propose to make clear that most disclosures that fall under paragraph (a)(1)(i) (*i.e.,* are for a purpose that would otherwise be subject to the accounting) but that are also required by law do not require an accounting. For example, if a disclosure to a public health authority or for workers' compensation is required by law (rather than merely authorized by law), then the covered entity or business associate is not required to include such a disclosure in a requested accounting. We propose, however, that covered entities and business associates account

for disclosures for judicial and administrative proceedings and for law enforcement purposes, even when such disclosures are required by law. This is consistent with our general treatment of such disclosures under § 164.512(a)(2), where we provide that a disclosure that is required by law but that also falls within the law enforcement or judicial and administrative proceeding provisions at § 164.512(e) and (f) must meet the latter's requirements. As indicated above, we believe that disclosures for law enforcement purposes and judicial and administrative proceedings directly implicate an individual's legal and/or personal interests and thus believe the individual should have a right to learn of such disclosures.

If a covered entity has been subject to the Privacy Rule for less than three years, then the covered entity only need account for the period of time during which the covered entity was subject to the Rule.

2. Implementation Specification: Content of the Accounting

Currently, the Privacy Rule at § 164.528(b)(2) requires an accounting of disclosures to include the date of disclosure, name and (if known) address of the recipient, a brief description of the type of protected health information disclosed, and a brief statement of the purpose of the disclosure. We are proposing to maintain these elements, but with some minor modifications.

We are proposing at paragraph (a)(2)(i)(A) that a covered entity or business associate need only provide an approximate date or period of time for each disclosure, if the actual date is not known. At a minimum, the approximate date must include a 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. Thus, the accounting may include the specific date of a disclosure (*e.g.,* December 1, 2010), a month and year (*e.g.,* December 2010), or an approximate time range (*e.g.,* between December 1, 2010 and December 15, 2010).

The Privacy Rule currently provides, at § 164.528(b)(3), that for multiple disclosures of protected health information to the same person or entity for the same purpose, the accounting may provide all of the information required by paragraph (b)(2) for the first disclosure; the frequency, periodicity, or number of disclosures during the accounting period; and the date of the last disclosure. We instead propose that, for multiple disclosures to the same person or entity for the same purpose, the approximate period of time is sufficient (*e.g.,* for numerous disclosures, "December 2010 through August 2011," or "monthly between December 2010 and present"). An exact start date and end date would not be required.

Note that, under our proposal, a time period of multiple months is permitted for multiple disclosures to the same recipient for the same purpose, but not a single disclosure. Accordingly, a single disclosure in February 2010 could not be described as "between January 2010 and May 2010." In contrast, three disclosures that began in January 2010 and ended in May 2010 could be described as "between January 2010 and May 2010."

Further, we clarify that the date of disclosure may be descriptive, rather than a specific date. For example, the accounting may provide that a disclosure to a public health authority was "within 15 days of discharge" or "the fifth day of the month following discharge."

We propose at paragraph (a)(2)(i)(B) that the accounting must include the name of the entity or natural person who received the protected health information and, if known, their address. This conforms to the current regulatory language. We are proposing an exception, however, for when providing the name of the recipient would itself represent a disclosure of protected health information about another individual. For example, if a physician's office mistakenly sends an appointment reminder to the wrong patient (and determines that the impermissible disclosure does not require breach notification because it does not compromise the privacy or security of the information), then the accounting may indicate that the disclosure was to "another patient." We believe that the alternative of providing the name of the recipient in this example would unnecessarily disclose the protected health information of the recipient by demonstrating that the recipient is also a patient of the physician practice.

As with the current accounting requirement of the Privacy Rule, we are proposing at paragraph (a)(2)(i)(C) that the accounting must include a brief description of the protected health information that was disclosed. We have proposed a slight revision to the regulatory language, replacing "a brief description of the protected health information disclosed" with "a brief description of the type of protected health information disclosed." This change is intended to reflect that the accounting is only required to provide information about the types of protected health information that were the subject of the disclosure.

We are proposing at paragraph (a)(2)(i)(D) that the accounting include a brief description of the purpose of the disclosure. We are proposing to change the current language from "statement" to "description" to make clear that only a minimum description is required if it reasonably informs the individual of the purpose. For example, "for public health" or "in response to law enforcement request" is sufficient. We propose to retain the language indicating that a copy of a written request may be substituted for a description of the purpose of the disclosure. When a written request provides more information than the description in the accounting, we encourage the covered entity to provide a copy of the request to better inform the individual of the circumstances surrounding the disclosure.

Although individuals would have a right to an accounting of all of the included disclosures occurring within the three years prior to the request, in paragraph (a)(2)(ii) we propose to require that covered entities provide individuals the option of limiting the accounting to a particular time period, type of disclosure, or recipient. We believe that such options are in the best interests of both the individual and the covered entity. Often, individuals are only interested in learning of disclosures that occurred over a limited period of time, such as a particular episode of care or within the past few months. In such cases, the individual is not well served by receiving an accounting that covers three years. Similarly, if an individual is only interested in learning of whether certain types of disclosures have been made (such as to law enforcement) or if a particular person or entity received the individual's information, then it is in both the individual's and covered entity's interests to limit the accounting to the relevant information.

Additionally, as in the current Privacy Rule, an individual may be required to pay for an accounting of disclosures if the covered entity has already provided the individual with an accounting within the prior twelve months. The individual should not have to pay for an accounting report that covers a three-year period if the individual is trying to learn of disclosures that occurred over a more limited period of time. Similarly, we expect that a covered entity can significantly reduce the cost of generating an accounting of disclosures by narrowing the scope of the report to

that which is of interest to the individual.

Covered entities are permitted to also offer other options to individuals for how to limit an accounting request. For example, a covered entity may provide the individual with the option to limit the accounting of disclosures to disclosures by a specific organization, such as disclosures by the covered entity or disclosures by a particular business associate.[3]

3. Implementation Specification: Provision of Accounting

In paragraph (a)(3), we are proposing requirements regarding the provision of an accounting of disclosures, such as the timeframe for providing the accounting, the form of the request, and permissible charges for an accounting. We are proposing three modifications to the existing regulatory requirements: (a) Decreasing the permissible response time from 60 days to 30 days; (b) requiring that covered entities provide individuals with the accounting in the form and format requested by the individual if readily producible (*e.g.,* an electronic copy of the accounting); and (c) clarifying that the covered entity may require the individual to submit the accounting request in writing.

We are proposing to reduce the timeframe for responding to an accounting from 60 days to 30 days. While we have received anecdotal evidence that responding to an accounting request may take a significant number of hours, we have not received information suggesting that it normally takes more than 30 days to respond. Additionally, because we are reducing the scope of the accounting to designated record set information and the length to three years, we believe that a 30-day period is appropriate. In the rare cases where it may take more than 30 days to respond, we are proposing to retain the availability of a 30-day extension. We request comment on 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 covered entities. Specifically, we request comment on how long covered entities have needed to collect the information necessary for an accounting (including from business associates) and to generate an accounting of disclosures.

Additionally, we are proposing that the covered entity must provide individuals with the accounting in the form (*e.g.,* paper or electronic) and format (*e.g.,* compatibility with a specific software application) requested by the individual if readily producible in such form and format. We expect that many individuals will prefer an electronic copy of an accounting, especially if the accounting includes a large number of disclosures or if the individual may be charged for the accounting and an electronic copy would cost less. If an individual requests the accounting in electronic form and the covered entity is readily able to produce an electronic accounting, then the covered entity must do so. Additionally, if an individual requests a particular format, such as a PDF file or a format compatible with a particular word processor, the covered entity should provide the accounting in such format if readily producible. If the requested form and format is not readily producible, then a covered entity may provide a hard copy of the accounting or the parties may try to determine if another form and format is acceptable. Unlike the access report discussed below, we do not propose to require that the accounting of disclosures be provided in electronic form, unless it is readily producible in such form, because we understand that generating an accounting for disclosures is still a very manual process and the accounting provision applies to both electronic and paper records. However, where covered entities are able to do so (and the individual has not specifically requested a paper copy), we strongly encourage them to provide the individual with a machine readable or other electronic copy of the accounting. As explained further below, we consider machine readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer. We request comment on the burdens associated with providing electronic formats as requested by individuals, machine readable or otherwise.

As with other communications to the individual, the covered entity must implement reasonable and appropriate safeguards to deliver a copy of the accounting to the individual. However, what is reasonable and appropriate will vary based on the capabilities of the covered entity and the preferences of the individual. If the individual asks for an electronic copy of the accounting but does not want the file to be encrypted or password protected, then the covered entity should provide the electronic copy without such protections. The covered entity is not responsible or liable for the information once it is in the individual's possession.

We also propose to clarify that a covered entity may require individuals to make a request for an accounting in writing (which includes electronic requests) provided that the covered entity informs individuals of such a requirement. This same language is currently found in § 164.524 (access of individuals to protected health information) and § 164.526 (amendment of protected health information). We encourage covered entities to create forms for individuals to request an accounting that inform individuals of the information that will be included and allow individuals to narrow the request based on their interests (such as by allowing individuals to request disclosures over a certain period of time, to a certain recipient, or for a certain purpose). We believe that it is in both the covered entity's and individual's best interests to use written requests to narrow accountings, so that the individual only receives the information of interest, and the covered entity does not have the administrative burden of responding to overly broad requests.

Finally, we continue to provide that the covered entity may not charge for the first request for an accounting in a 12-month period, but may charge a reasonable and cost-based fee for providing an accounting in response to subsequent requests in the 12-month period (which may include the reasonable costs of including disclosures by business associates). The proposed rule requires the covered entity to inform the individual at the time of the first accounting request that all subsequent requests in the 12-month period may be subject to a fee. The proposed rule also requires the covered entity to inform the individual of the fee at the time of the subsequent request and to provide the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

4. Implementation Specification: Law Enforcement and Health Oversight Delay

In paragraph (a)(4), we are proposing to retain the requirement for covered entities to delay the provision of an accounting of disclosures based on an ongoing law enforcement investigation.

[3] We note that proposed § 164.528(b)(2)(ii), discussed below, specifically states that a covered entity may provide the individual with the option to limit the access report to a specific organization. We have not included similar language in the accounting provision because we expect it will be less likely that individuals will be interested in limiting their accounting requests in this fashion. The lack of this regulatory language in § 164.528(a)(2)(ii) should not be interpreted as prohibiting covered entities from offering individuals the option to limit their accounting request by organization.

This request for delay by law enforcement is not subject to challenge. We also clarify in the proposed rule that if law enforcement requests a delay, a covered entity shall still account for all other disclosures in accordance with § 164.528(a) and shall supplement the accounting with information about the law enforcement disclosures upon expiration of the requested law enforcement delay. We propose to no longer include a delay for a health oversight investigation since we are proposing that disclosures for health oversight activities are no longer subject to the accounting requirements.

5. Implementation Specification: Documentation

We propose at paragraph (a)(5) to revise the documentation requirements for the accounting of disclosures. The current rule provides that covered entities must document and retain the information necessary to generate an accounting of disclosures, a copy of the written accounting that is provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals in accordance with § 164.530(j). Section 164.530(j)(1)(ii) provides that if the Privacy Rule requires a communication to be in writing, then the covered entity must maintain the writing or an electronic copy of the writing as documentation. Similarly, § 164.530(j)(1)(iii) provides that if the Privacy Rule requires an action, activity, or designation to be documented, then the covered entity must maintain a written or electronic record of such action, activity, or designation. Section 164.530(j)(2) provides that any documentation required under § 164.530(j)(1) be retained for six years from the date of its creation or the date when it was last in effect, whichever is later. Accordingly, under the current rule, a covered entity must maintain for six years the information necessary to generate an accounting of disclosures, the written accounting that is provided to an individual, and the designation of the persons or offices responsible for receiving and processing accounting requests. In the case of the designation of who is responsible for handling accounting requests, the covered entity must retain the designation for six years from the date when it was last in effect.

We are proposing two changes to the documentation requirements. First, because we are proposing to reduce the accounting period from six years to three years, we do not believe there is a need to retain information that is solely being retained in order to provide an accounting of disclosures for more than three years. Of course, covered entities and business associates may choose to retain this information longer based on other legal requirements or internal policies. Second, we are revising the regulatory language to clarify that a covered entity must retain a copy of the accounting provided to the individual, and not the original accounting document. Accordingly, under the proposed rule, a covered entity must maintain the documentation necessary to generate an accounting of disclosures for three years (rather than for the six-year retention period that is set forth at § 164.530(j)), 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.

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

1. Standard: Right to an Access Report

In addition to the right to an accounting of disclosures, we are proposing to provide individuals with a right to receive an access report that indicates who has accessed their electronic designated record set information (this right does not extend to access to paper records). In the below discussion of the proposed right to an access report, we refer to both "access logs" and "access reports." For purposes of this discussion, the access log is the raw data that an electronic system containing protected health information collects each time a user (as the term is defined in the Security Rule at § 164.304) accesses information. The access report is a document that a system administrator or other appropriate person generates from the access log in a format that is understandable to the individual.

We note that an access log also may commonly be referred to as an "audit trail" or "audit log" and an access report is similar to an "audit report." We do not use the terms audit trail or audit log in order to distinguish the access report from documents that are generated by organizations for their internal auditing purposes.

We also note that a covered entity will usually have electronic designated record set information in multiple systems which each maintain separate access logs. Our expectation is that data from each access log will be gathered and aggregated to generate a single access report (including data from business associates' systems).

This proposed right to an access report would implement section 13405(c) of the HITECH Act by providing individuals with information about disclosures through an electronic health record (EHR) for treatment, payment, and health care operations. While the HITECH Act provision only addresses "disclosures" and refers to an EHR, we are exercising our discretion under the more general HIPAA statute to expand this right to uses of information (*e.g.,* electronic access by members of a covered entity's or business associate's workforce) and to all electronic protected health information about an individual in any designated record set. We note that this access report will not encompass all electronic disclosures of protected health information for purposes of treatment, payment, and health care operations. Section 13405(c) is limited to disclosures "through an electronic health record" and does not encompass electronic disclosures outside of the EHR. Similarly, the proposed access report will capture information each time electronic protected health information in a designated record set information is accessed, and therefore will capture each disclosure through an electronic designated record set (by capturing information about who accessed the electronic designated record set), but will not capture electronic disclosures of protected health information that occur outside of electronic designated record set systems.

We propose to expand this privacy right beyond the statutory provision for a number of reasons. First, we believe that individuals are interested in learning who has accessed their information without regard to whether the access is internal (a use) or by a person outside the covered entity and its business associates (a disclosure). We believe that the inclusion of both uses and disclosures in the access report significantly increases the benefits to individuals by providing a more complete picture of who has accessed their information. We do not believe that the inclusion of "uses" of designated record set information in the access report represents an unreasonable burden on covered entities and business associates. In response to our RFI, most covered entity commenters indicated that their system is unable to automatically distinguish between uses and disclosures of information. Accordingly, the inclusion of all access, rather than only access that represents a disclosure, may actually be

less burdensome on covered entities and business associates than the alternative of configuring systems to distinguish between uses and disclosures of information.

We have included all electronic protected health information in a designated record set, rather than only EHR information, because we believe that this greatly improves transparency and better facilitates compliance and enforcement, while placing a reasonable burden on covered entities and business associates. As discussed below, in accordance with the Security Rule, all electronic systems with designated record set information should be creating access logs with sufficient information to create an access report. Regardless of whether the system qualifies as an EHR, we believe that it is reasonable to provide this access log information to individuals upon their requests. We propose to limit the access report requirements to electronic protected health information because we believe that extending the right to paper records would place an unreasonable administrative burden on covered entities since tracking such access is not an automated process and is not currently required under the Security Rule.

We believe that this broader approach adds clarity to compliance and enforcement efforts by avoiding the need to categorize certain electronic systems as EHRs. As health information technology advances, the concept of what constitutes an EHR is in a state of flux. A large integrated delivery system may have a large number of electronic systems containing designated record set information and there is no consensus on which of those systems should be considered part of the EHR. For example, a system may not be considered part of an EHR for purposes of Medicare and Medicaid's meaningful use Stage 1, but may become part of the EHR under Stages 2 or 3. We believe that limiting the right to an access report to an EHR would create too much confusion for covered entities, hinder our enforcement efforts, and lead to confusion for individuals who seek to exercise their privacy rights.

We recognize that our proposal extends the right to an access report to all covered entities and business associates that maintain electronic designated record set information, including covered entities and business associates that do not have systems that could be categorized as EHRs. We believe that this is reasonable since all such covered entities and business associates are required by the Security Rule to maintain access logs and, therefore, should be able to provide this information to individuals in response to requests.

We believe that the administrative burden on covered entities who are complying with the HIPAA Security Rule will be reasonable, in light of their existing obligation to log access to electronic protected health information. Section 164.312(b) of the Security Rule (Standard: Audit Controls) currently requires 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." Therefore, systems with designated record set information should already be configured to record activities such as when users access information. Additionally, § 164.308(a)(1)(ii)(D) of the Security Rule (Implementation specification: Information system activity review) currently requires covered entities to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." Accordingly, covered entities should already be logging access to electronic protected health information and regularly reviewing reports of such access.

We also propose to require covered entities to furnish access reports for business associates that maintain designated record set information. Individuals may have the same interest in learning who, at a business associate, has accessed their information (especially if the individual knows someone employed by the business associate). In response to a request for an access report, a covered entity must contact the business associates that create, receive, maintain, or transmit electronic designated record set information and obtain from them access reports with respect to the individual's information. As with accounting for disclosures under proposed paragraph (a), a covered entity only needs to obtain information from business associates that handle designated record set information (in this case, electronic designated record set information). Based on our proposed accounting and access report provisions, and the current provision at § 164.504(e)(ii) that requires business associates to make available protected health information in accordance with §§ 164.524 and 164.526 (which are both limited to designated record set information), we recommend that covered entities track which of their business associates have designated record set information.

We do not believe that the proposed language will place an unreasonable burden on business associates. Under § 164.314(a)(2)(i)(A) of the current Security Rule, covered entities are required to include in their business associate agreements the requirement that the business associates maintain reasonable and appropriate administrative, physical, and technical safeguards for electronic protected health information. Such safeguards should include the ability to determine who has accessed electronic protected health information. Furthermore, section 13401(a) of the HITECH Act specifically requires business associates to comply with §§ 164.308 (administrative safeguards) and 164.312 (technical safeguards) of the Security Rule. *See also* 75 FR 40,868, July 14, 2010 (proposing regulatory amendments to the Security Rule to require business associates to comply with the Rule). Accordingly, as with covered entities, business associates should have the ability to create an access report that indicates who has accessed an individual's electronic designated record set information.

We note that section 13405(c)(3) of the HITECH Act specifies that a covered entity may provide either an accounting that includes disclosures by business associates or an accounting that is limited to its own disclosures and a list of business associates (with contact information for each business associate). Under the second option, the individual would then need to contact each business associate to learn of any disclosures. We believe that the second option places an undue burden on the individual. First, the individual generally will not have a relationship with many of the business associates and therefore may feel uncomfortable contacting them. Second, some of the business associates may not even have designated record set information and thus may have no information to provide to the individual. Accordingly, we are exercising our general authority under the HIPAA statute to propose that the covered entity's access report include uses and disclosures by business associates of electronic designated record set information maintained by the business associates, rather than merely providing a listing of business associates.

2. Implementation Specification: Content of the Access Report

In paragraph (b)(2), we propose that the access report must set forth: (a) The date of access; (b) the time of access; (c) the name of the natural person, if available, otherwise the name of the

entity accessing the electronic designated record set information; (d) a description of what information was accessed, if available; and (e) a description of the action by the user, if available (*e.g.,* "create," "modify," "access," or "delete"). We expect that any access report will be readily capable of providing the date and time of access and the user name, and in many cases can also provide information about what information was accessed and the user's action (such as create, modify, print, *etc.*).

Our proposal would require the access report to include the date and time of access. We expect that all access logs include this information, so we believe it should be readily available for inclusion in access reports without substantial burden to covered entities and business associates. We note that access logs will sometimes include both the start time and end time for access. We intend for the covered entity to include the start time in the access report, although covered entities are free to also include the end time when it is available.

We propose to require that covered entities include in the access report the name of the natural person who is accessing the information, if available. We recognize that some access logs may not provide the first and last name of the person accessing the information, but instead may rely on a user ID. In such cases we expect, however, that a covered entity can readily match a user ID with a first and last name. We do not propose specific requirements as to how covered entities create their access reports. Accordingly, a covered entity is free to modify their systems (if necessary) to readily produce the first and last name of each user who accesses designated record set information, or may instead choose to perform a match between each user ID and name only in response to a request for an access report.

We note that in some circumstances an access log may only capture the name of an entity, rather than a natural person. For example, when information from an EHR is exchanged with an organization outside of the covered entity, the access log may capture only the name of the organization receiving the information. In such cases, when the name of a natural person is unavailable, the name of an entity that is outside of the covered entity or business associate will suffice.

Additionally, we recognize that an electronic designated record set system may exchange data with another electronic system within the organization. In such cases, we would permit the access log to identify such access by the name of the covered entity in order to reflect that the individual's information was accessed by one of the covered entity's systems. To the extent that the covered entity is able to provide more information, such as a description of the system that is accessing the information, we encourage covered entities to include such information. We recognize that more information than the covered entity's name would be helpful to the individual, but we have concerns about the burden on covered entities if they were to have to describe each internal exchange of information between systems in more detail. In contrast, we believe individuals' interest in such internal exchanges may be limited. We request comment on this issue, particularly the burden of providing identifying information about internal systems and the interests of individuals in learning of such internal exchanges.

We are proposing to include the requirement that an access report include a description of what information in the electronic designated record set was accessed, if this information is available. We recognize that only some access logs may collect this information, and we are not proposing at this time to require covered entities and business associates to revise their remaining systems to collect this data going forward. We note that, because an access report will often reflect the access logs of various systems, an access report may include some entries that identify what information was accessed, while other entries may leave this field blank.

While we recognize that it may be helpful to individuals to learn what information was accessed, we believe that it would be unreasonable to require all covered entities and business associates to modify all of their electronic designated record set systems to collect this information, especially in light of the relatively small number of accounting requests that most covered entities have received to date. We request comment on the availability of this information in current access logs, the importance of the information to individuals, and the potential administrative burden of requiring that access reports include a description of what information was accessed.

Lastly, we propose to require that the access report include a general description of the action taken by the user with respect to the record, if available, such as whether the user created, modified, deleted, or merely accessed the record. This provision is not intended to require covered entities and business associates to include in the access report a description of what use or disclosure was ultimately made with the information accessed or to whom the user provided the information. For example, the access report should not indicate that the user provided a copy of the record to law enforcement.

Unlike an accounting under paragraph (a) of this section, the access report need not include the address of the user (required under paragraph (a) when known) or a brief statement of the purpose of the disclosure. Section 13405(c) of the HITECH Act provides that the Secretary shall only require the collection of information after taking into account the interests of individuals in learning the circumstances under which their protected health information is being disclosed and the administrative burden of accounting for such disclosures. After consideration of our experience in administering the Privacy Rule and the feedback we received from stakeholders over the years and in response to our RFI, we do not propose to require these elements in an access report because we believe that the burden of collecting them outweighs the interests of individuals in learning of them.

We are not requiring access reports to include the address of the user because we do not believe that this information is uniformly collected by current access logs and do not believe that individuals have sufficient interest in this information to warrant adding it. While some access to electronic designated set information will occur outside of a covered entity's facility (including access granted to persons who are not members of the covered entity's workforce) we expect that most access occurs at the covered entity's facility, meaning that the address would be that of the facility. We do not expect that most individuals have a strong interest in learning where their information was accessed, especially where it is mostly accessed at the facility. Rather, we expect that individuals are far more interested in learning who accessed their information rather than where it was accessed. We request comment on the potential burden to covered entities and potential benefit to individuals of requiring the access report to include address information that indicates where the access occurred.

We are not proposing to require that access reports include a description of the purpose of the access. In response to our RFI, a majority of commenters indicated that we should not require that an accounting of disclosures for treatment, payment, and health care operations include the purpose of the

disclosure. Commenters stated that this information is not currently captured when protected health information is accessed, and requiring the information would represent a significant disruption of workflow. The majority of commenters also indicated that individuals did not have a good understanding of terms such as "health care operations." A minority of commenters (approximately 20%, representing consumers and covered entities) indicated that inclusion of the purpose of the disclosure is essential to a meaningful accounting. In addition to the RFI, we have received anecdotal reports that identifying the purpose of a disclosure is sometimes important, but that more often individuals are most interested in learning who has accessed their information.

After consideration of the input that we received in response to the RFI and our experience in administering the Privacy Rule, we believe the burden on covered entities and business associates in identifying the purpose of each access to electronic designated record set information significantly outweighs the benefit to individuals of learning of such information. In almost all cases, covered entities and business associates would need to modify existing systems in order to add the ability to track why a user is accessing electronic designated record set information. These modifications would represent significant time and cost. Once the modifications are made, requiring users to input their reason for accessing electronic protected health information would represent a significant disruption to existing workflow. The cumulative effect of requiring an extra step each time a user accesses electronic designated record set information would be substantial. Furthermore, because there would be no similar requirement to track the reason each time paper records are viewed, such a proposal could represent a significant disincentive to adoption of EHR technology.

In contrast to the burden on all covered entities and business associates, we believe the benefit to individuals would be modest. To date, we understand there have been relatively few requests for accountings of disclosures. While the availability of access reports may lead to an increased number of requests, we would continue to expect that only a small minority of individuals would exercise this right. Of those requests, we expect that many individuals would only be interested in learning who accessed their information, without regard to why the information was accessed. Accordingly, with respect to tracking the purpose of each access to electronic designated record set information, we believe that the substantial burden on all covered entities and business associates significantly outweighs the benefits to a relatively small number of individuals who would seek to find out why their information was accessed. We note that, with respect to the disclosures that we believe to be of most interest to individuals (such as impermissible disclosures for which the individual did not receive breach notification or disclosures to law enforcement of designated record set information), the individual would have the right to a full accounting under paragraph (a). We request comment on our proposal to not require covered entities and business associates to include a description of the purpose of access in access reports.

We note that we have not proposed that the access report include the ultimate recipient of the electronic protected health information, unless the recipient is the natural person or entity with direct access to the electronic protected health information (see clarification above regarding documenting action by the user in the access report). We believe that this information, as well as the purpose of the access, is generally not captured by systems currently available today. As such, we have not proposed the same exceptions as for the accounting of disclosures requirement (*e.g.,* for a law enforcement delay, or for reports to a government agency of suspected child abuse), since information that may merit an exception would not be included within the access report.[4] Even if such exceptions were included, it is not clear to us that there would be a practical way in which to identify the excepted accesses in order to exclude them from the access report, again because the purpose and ultimate recipient are not recorded. We request comment on our assumption that systems do not record information about the purpose of the access and ultimate recipient of the information within audit logs. We additionally request comment on ways in which such accesses, if excepted from the access report, could be identified and excluded in an automated way.

Based on the above, we expect that the proposed right to an access report will require minimal, if any, changes to existing information systems. Covered entities and business associates who are compliant with the Security Rule or their business associate agreements should already be logging the information necessary for an access report and should be able to generate such a report. As noted earlier, we recognize that electronic designated record set information will often reside in a number of distinct systems that maintain separate access logs. There may be significant burden in aggregating this data into a single access report. However, we believe that this administrative burden is reasonable in light of the interests of individuals in learning who has accessed their protected health information. Additionally, the burden of generating access reports will be directly proportionate to the interests of individuals; if few individuals request access reports, then covered entities will rarely need to undertake the burden of generating an access report. We request comment on the above conclusions.

In paragraph (b)(2)(ii), we are proposing to require covered entities to provide individuals with the option to limit the access report to a specific date, time period, or person. For example, an individual may request that the access report be limited to whether a specific person (such as a family member) accessed the individual's electronic designated record set information over a specific time period (such as within the last two months). We believe that this requirement will prove beneficial to both individuals and covered entities. It will be beneficial to individuals by allowing them to better focus on information of interest. If an individual is only interested in learning of whether a particular person accessed the individual's health information over a specific time period, there is no reason for the individual to receive a voluminous access report filled with other information.

Similarly, we believe this requirement will prove beneficial to covered entities by minimizing the information that the covered entities need to collect. We expect that audit systems can readily produce an access report limited in this fashion. Therefore, we believe that it would be an unnecessary use of the covered entity's and business associates' resources to create a broad access report when the individual is only seeking very specific information.

We are recommending—although not requiring—that covered entities offer individuals the option to limit the access report to specific organizations. For example, if the individual is not interested in learning of access at

[4] We note that to the extent a covered entity nonetheless has a reasonable belief that providing certain information in the access report to a personal representative of an individual could endanger the individual, it may elect not to provide the information pursuant to § 164.502(g)(5) of the Privacy Rule.

business associates, there is no reason for the covered entity to contact business associates to obtain their access reports. Conversely, if the individual is interested in learning about access at a particular business associate, then the covered entity need not run an internal access report nor obtain access reports from business associates other than the one that is of interest to the individual.

We are also proposing, in paragraph (b)(2)(iii), that the covered entity provide the access report in a format that is understandable to the individual. This would be a format that is structured in a manner so that it reasonably can be understood by individuals without an external aid. This proposal does not require any summary information or additional content, such as information about the role of each person who accesses the individual's protected health information.

The following is an example of an access report that is formatted so as to be understandable to the individual:

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

In contrast, the following is the same information that is not in a format that is understandable to the individual:

201110101430JOHNANDREW3

The above is not understandable because it is coded and requires the use of an external guide.

3. Implementation Specification: Provision of the Access Report

We are proposing at paragraph (b)(3)(i) the same timing requirements for provision of an access report as for provision of an accounting of disclosures. Accordingly, a covered entity would have 30 days to provide the access report, including the logs of business associates that create, receive, maintain or transmit electronic designated record set information. The covered entity may extend the time by 30 days where necessary, as long as the covered entity provides the individual with a written statement that includes the reason for the delay and the date by which the covered entity will provide the access report. The covered entity is only permitted one extension of time.

We are proposing at paragraph (b)(3)(ii) that the covered entity must provide the access report in the machine readable or other electronic form and format (*e.g.,* compatibility with a specific software application) requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. If the individual does not agree to accept the readable electronic format that is readily producible by the covered entity, the covered entity may provide a readable hard copy. If the individual requests the access report in hard copy form, the covered entity must provide the individual with the access report in a readable hard copy form. For these purposes, we propose to provide that machine readable data is digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the access report in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats. We request comment on the ability of covered entities to provide access reports in machine readable or other electronic formats.

As with the accounting of disclosures, we are proposing that the covered entity may not charge for providing the first access report to an individual in any 12-month period, but may charge a reasonable, cost-based amount for each additional access report that is requested within the 12-month period (which may include the reasonable costs of including access report information of business associates). The proposed rule requires the covered entity to inform the individual at the time of the first access report request that all subsequent requests in the 12-month period may be subject to a fee. The proposed rule also requires the covered entity to inform the individual of the fee at the time of the subsequent request and to provide the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

We are also proposing, in paragraph (b)(3)(iv), that the covered entity may require individuals to make requests for an access report in writing provided that it informs the individual of such a requirement. This same language is currently found in § 164.524 (access of individuals to protected health information) and § 164.526 (amendment of protected health information). As we discussed with respect to the provision of the accounting of disclosures, we encourage covered entities to create forms for individuals to request an access report that provides information about the information the individual will receive and allows the individual to narrow the request based on the individual's interests. We believe that it is in both the covered entity's and individual's best interests to use written requests to narrow access reports, so that the individual only receives the information of interest, and the covered entity does not have the administrative burden of responding to an overly broad request.

4. Implementation Specification: Documentation

We are proposing at paragraph (b)(4) the same documentation requirements for access reports as for accountings of disclosures. Accordingly, we propose that a covered entity or business associate must retain the documentation needed to produce an access report (*e.g.,* the necessary access log) for three years (rather than for the six-year retention period that is set forth at § 164.530(j)), the covered entity must retain for six years copies of access reports that were provided to individuals, and must maintain a designation of the persons or offices responsible for receiving and processing requests for access reports for six years from the last date the designation was in effect.

5. Accounting for Disclosures That Are Made Through Electronic Health Information Exchange

In addition to the right to an access report, we also considered providing individuals with the right to receive a full accounting for treatment, payment, and health care operations disclosures through an EHR when such disclosures are made through electronic health information exchange (*i.e.,* disclosures that originate from an EHR that are received by another electronic system). For example, such a proposal would have required a full accounting, including a description of the purpose of the disclosure, when a covered entity or business associate transmits some or all of an EHR to another electronic system (such as another covered entity's EHR, a pharmacy, laboratory, or health plan). This would have included health information exchange when the disclosure is in response to a query, and health information exchange that is initiated by the disclosing covered entity.

After careful consideration of this option, we concluded that accounting for such disclosures at this time would be overly burdensome when compared to the potential benefit to individuals. Especially for EHR technology that is not certified pursuant to ONC standards and certification criteria, covered entities might need to make substantial and costly modifications to their existing EHR systems in order to track the purpose of disclosures for treatment, payment, and health care operations.

However, as electronic health information exchange expands and standards for such exchange are adopted, we intend to work with ONC to assess whether such standards should include information about the purpose of each exchange transaction. Adoption of such standards may significantly reduce the burden on covered entities to account for treatment, payment, and health care operations disclosures through electronic health information exchange. We then intend to revisit this issue and determine whether the accounting requirements should be revised to encompass such disclosures, in light of the interests of individuals and the reduced burden on covered entities.

We note that, despite not proposing to adopt the above option with respect to treatment, payment, and health care operations disclosures, individuals still have a right to learn of disclosures through electronic health information exchange if such disclosures fall under proposed paragraph (a)(1), such as disclosures for public health. Additionally, each time electronic designated record set information is accessed for purposes of electronic health information exchange (regardless of the purpose of the exchange), the date, time, and identity of the user will be captured in the access report.

C. Confidentiality of Patient Safety Work Product

We recognize that there may be times when a covered entity or business associate may disclose electronic designated record set information to a patient safety organization pursuant to the Patient Safety and Quality Improvement Rule at 42 CFR part 3, which implements the Patient Safety and Quality Improvement Act of 2005.

A member of a covered entity's or business associate's workforce may access electronic designated record set information for patient safety activities under 42 CFR part 3, or a covered entity may permit employees of a patient safety organization to directly access electronic designated record set information. The fact that a workforce member or other appropriate person uses or discloses protected health information for patient safety activities may constitute patient safety work product under 42 CFR part 3, and thus may fall under the privilege and confidentiality provisions of the Patient Safety and Quality Improvement Rule. It is not our intention to interfere with those protections.

Accordingly, we propose at paragraph (c) that a covered entity shall exclude from an accounting or access report under § 164.528 any information that meets the definition of patient safety work product at 42 CFR 3.20. This will avoid any conflicts between the two sets of regulations.

D. Notice of Privacy Practices—Section 164.520

Under the Privacy Rule at § 164.520, a covered entity is required to provide an individual with a notice of privacy practices that includes descriptions of the individual's rights under the Privacy Rule. Section 164.520(b)(1)(iv)(E) provides that the notice must contain a statement of the individual's right to receive an accounting of disclosures of protected health information as provided by § 164.528. We are proposing to revise § 164.520(b)(1)(iv)(E) to also require a statement regarding an individual's right under the proposed rule to receive an access report.

This proposed change to a covered entity's notice of privacy practices would constitute a material change to the notice. Section 164.520(b)(3) requires covered entities to promptly revise and distribute the notice as outlined in § 164.520(c) where there is a material change to the notice. With respect to health care providers with a direct treatment relationship with individuals, § 164.520(c)(2)(iv) requires the provider to make the notice available upon request on or after the effective date of the revision and, if the provider maintains a physical service delivery site, promptly have the notice posted and available at the delivery site for individuals to take with them. Health plans are currently required by the Privacy Rule to distribute notices to current members within 60 days of a material revision.

As discussed below in Section V, we are not proposing to require covered entities and business associates to comply with the access report requirements until January 1, 2013, or January 1, 2014, depending on the age of their electronic designated record set systems. Therefore, covered entities need not revise their notices of privacy practices to reflect the right to receive an access report until the earliest applicable compliance date.

We recognize that health plans may incur significant costs informing individuals of a change to their notices of privacy practices within 60 days of the effective date of the change. In the Department's notice of proposed rulemaking to implement the privacy provisions of the Genetic Information Nondiscrimination Act of 2008 (GINA) (74 FR 51703–51704) and its HITECH Act notice of proposed rulemaking (75 FR 40898–40899), the Department solicited comment on ways to inform individuals of changes to privacy practices without unduly burdening health plans. The Department has been considering a number of options in response to those comments, including allowing health plans to notify individuals of revisions to the notice of privacy practices (either by providing the revised notice or information about the material change and how to obtain the revised notice) in their next annual mailing to individuals then covered by the plan, rather than within 60 days of the material change. Any modifications to the 60-day time period for health plans will be addressed in those final rules. If any changes are made to the 60-day time period, it is expected that the change would then also apply to this rule when final.

However, even if the 60-day deadline to inform individuals of material changes is not modified by the Department in the other HITECH Act and/or GINA rulemakings, we believe that the cost to health plans to revise and distribute notices under this rule can be minimized in light of the lengthy compliance period we are considering. For example, a health plan can minimize its mailing costs by including notice of the new right to an access report in an annual mailing prior to the date that notification is required under § 164.520(c)(1)(i)(C) (i.e., prior to March 2, 2013, or 2014, the dates that are 60 days after the 2013 and 2014 compliance deadlines).

V. Effective and Compliance Dates

We propose separate compliance dates for the changes to the accounting of disclosures requirements and for the right to receive an access report. We propose that covered entities and business associates will be required to comply with the revised accounting of disclosures provision by no later than 180 days after the effective date of the final rule. The effective date of the final rule will be 60 days after publication in the **Federal Register**, so covered entities and business associates will have 240 days after publication of the final rule to come into compliance. This is consistent with our proposed changes to § 160.105 found in the notice of proposed rulemaking published at 75 FR 40,868, July 14, 2010. That proposal would establish at § 160.105 a 180-day compliance period for future modifications to the HIPAA Rules, unless otherwise specifically provided.

We believe that this compliance period is reasonable in light of current obligations on covered entities and business associates. For example, covered entities should currently be

able to produce an accounting of disclosures on request. Business associates should currently be able to provide accounting information to a covered entity on request. The proposed changes to the existing accounting for disclosures requirements generally would streamline the requirements and otherwise make compliance easier, as well as shorten the accounting period from six years to three years. Therefore, we expect that covered entities and business associates can implement these changes expeditiously.

We propose to require covered entities and business associates to produce an access report upon request beginning January 1, 2013, for any electronic designated record set systems that were acquired after January 1, 2009. Section 13405(c)(4)(B) of the HITECH Act provides that a covered entity that acquired an EHR after January 1, 2009, must account for disclosures for treatment, payment, and health care operations beginning January 1, 2011 (or the date that it acquires an EHR after January 1, 2011). The statute authorizes the Secretary to extend this date to no later than 2013. Because we are proposing to provide individuals with a right to an access report covering any electronic designated record set information, rather than only access to an EHR, we are basing the compliance date on when a covered entity acquires a particular electronic designated record set system. Additionally, because we recognize that covered entities will require time to create policies and procedures to generate an access report upon request, we are exercising our statutory authority and extending the 2011 date to January 1, 2013.

We propose to require covered entities and business associates to produce an access report upon request beginning January 1, 2014, for electronic designated record set systems that were acquired on or before January 1, 2009. Section 13405(c)(4)(A) provides that a covered entity that acquired an EHR as of January 1, 2009, must account for disclosures for treatment, payment, and health care operations beginning January 1, 2014. The statute authorizes the Secretary to extend this date to no later than 2016. For the same reasons as discussed above, we are making the compliance deadline contingent on when an electronic designated record set system was acquired. We do not believe that it is necessary to extend the January 1, 2014 date.

Covered entities and business associates should already be logging access to electronic protected health information and should have the ability to generate access reports pursuant to the Security Rule. We recognize that covered entities and business associates may need time to make some modifications to systems and processes, such as creating a process to aggregate data from multiple access logs into a single access report. However, we believe that the above dates of January 1, 2013, and January 1, 2014, will provide sufficient time. We note that this will also provide covered entities with time to revise their notices of privacy practices.

We recognize that, pursuant to these compliance dates, during 2013 a covered entity or business associate may be required to produce an access report that includes access to some electronic designated record set systems (those acquired after January 1, 2009) but not others (those acquired as of January 1, 2009). We encourage covered entities and business associates in such circumstances to provide access reports that include all designated record set systems during 2013, even if the covered entity or business associate is not required to include some of the electronic systems at that time.

Under our proposed rule, access reports must cover a three-year period and covered entities and business associates must retain their access log information for three years. Because covered entities should already be maintaining access logs pursuant to the Security Rule, we believe that it is reasonable to require covered entities to produce access reports, upon request, covering access over the prior three years beginning on the proposed January 1, 2013, and January 1, 2014, compliance dates. We request comment on whether covered entities will be able to generate access reports covering the preceding three years on these compliance dates.

VI. Regulatory Analyses

A. Introduction

We have prepared a regulatory impact statement in compliance with Executive Order 12866 (September 1993, Regulatory Planning and Review), the Regulatory Flexibility Act (RFA) (September 19, 1980, Pub. L. 96–354), the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4), and Executive Order 13132 on Federalism.

1. Executive Order 12866

Executive Orders 13563 and 12866 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action" although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget.

A regulatory impact analysis must be prepared for major rules that have economically significant effects ($100 million or more in any one year) or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal government or communities (58 FR 51741).

We estimate the effects of the requirement for covered entities (including indirect costs incurred by third party administrators, which frequently send out notices on behalf of health plans) to issue new notices of privacy practices, would result in new total costs of $20.2 million. We estimate that the private sector would bear almost the entirety of this new total cost, with State and Federal plans bearing a minimal share. While we anticipate the issuance of new notices of privacy practices to be the predominant source of additional costs for covered entities, there may be the potential for covered entities to incur other costs which we are unable to quantify at this time, as discussed further below. For example, we request more information on the number of anticipated accounting of disclosures and access reports; the additional costs, if any, of offering them in electronic formats (both machine readable or non machine readable); the burden of tracking access to electronic designated record set information; and any other additional changes to existing systems that would be necessary.

Although we expect the economic impact of issuing privacy notices and the possibility of other non-quantifiable costs and savings discussed in the regulatory analysis below to be less than $100 million annually, we nevertheless conducted analysis of the costs of the proposed regulations.

2. Regulatory Flexibility Act

The RFA requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities. We present our regulatory

flexibility analysis of this proposed rule in Section D below.

The RFA generally defines a "small entity" as (1) a proprietary firm meeting the size standards of the Small Business Administration (SBA), (2) a nonprofit organization that is not dominant in its field, or (3) a small government jurisdiction with a population of less than 50,000. Because 90 percent or more of all health care providers meet the SBA size standard for a small business or are nonprofit organizations, we generally treat all health care providers as small entities for purposes of performing a regulatory flexibility analysis. The SBA size standard for health care providers ranges between $7.0 million and $34.5 million in annual receipts.

With respect to health insurers and third party administrators, the SBA size standard is $7.0 million in annual receipts. While some insurers are classified as nonprofit, it is possible they are dominant in their market. For example, a number of Blue Cross/Blue Shield insurers are organized as nonprofit entities; yet they dominate the health insurance market in the States where they are licensed. In addition, we lack the detailed information on annual receipts for insurers and plan administrators and, therefore, we do not know how many firms qualify as small entities. We welcome comments on the number of small entities in the health insurer and health plan administrator market.

3. Unfunded Mandates Reform Act

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) requires that agencies assess anticipated costs and benefits before issuing any rule whose mandates would require spending in any one year of $100 million in 1995 dollars, updated annually for inflation. In 2010, that threshold is approximately $135 million. UMRA does not address the total cost of a rule. Rather, it focuses on certain categories of cost, mainly those "Federal mandate" costs resulting from: (1) Imposing enforceable duties on State, local, or tribal governments, or on the private sector; or (2) increasing the stringency of conditions in, or decreasing the funding of, State, local, or tribal governments under entitlement programs. We estimate the costs of the proposed rule will be approximately $20.2 million, largely due to the revision of privacy notices. This amount is not sufficient to warrant an analysis of costs and benefits under the UMRA provisions. However, as we explained under EO 12688, we are conducting an analysis of the costs that could result from the proposed rule.

4. Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications.

The Federalism implications of the Privacy and Security Rules were assessed as required by Executive Order 13132 and published as part of the preambles to the final rules on December 28, 2000 (65 FR 82462, 82797) and February 20, 2003 (68 FR 8334, 8373), respectively. Regarding preemption, the preamble to the final Privacy Rule explains that the HIPAA statute dictates the relationship between State law and Privacy Rule requirements, and the Rule's preemption provisions do not raise Federalism issues. The HITECH Act, at section 13421(a), provides that the HIPAA preemption provisions shall apply to the HITECH provisions and requirements.

We do not believe that this rule will impose substantial direct compliance costs on State and local governments that are not required by statute. The proposed rule would only apply to State and local government entities that are covered entities under the HIPAA Privacy and Security Rules. Such entities should already be maintaining access logs with the information necessary to generate an access report. Accordingly, the costs attributable to the new right to receive an access report should be limited to the cost of responding to requests for such a report (*e.g.*, the burden of aggregating information from multiple access logs into a single access report). This cost should be small, in light of the relatively small number of requests that we expect covered entities to receive from individuals.

State and local government entities that are covered entities may also incur some cost in revising their notices of privacy practices. Based on the length of time provided prior to the January 1, 2013, and January 1, 2014, compliance dates, we expect that such covered entities may minimize their costs by informing individuals of the change to the notice of privacy practices as part of an annual mailing.

In considering the principles in and requirements of Executive Order 13132, the Department has determined that these proposed modifications to the Privacy Rule will not significantly affect the rights, roles, and responsibilities of the States.

B. Why are we proposing these regulations?

Section 13405(c) of the HITECH Act directs the Secretary to promulgate regulations requiring covered entities to account for disclosures of protected health information through an EHR for purposes of treatment, payment, and health care operations. In issuing the regulations, the Secretary is to balance the burden imposed on covered entities with the interests of individuals to know about the disclosure of their protected health information.

We are proposing these regulations to provide individuals with the expanded right to an accounting that is provided for in section 13405(c), to provide individuals with a more complete accounting through the right to receive an access report that includes information on each time a covered entity's or business associate's electronic designated record set information is accessed, and to improve the workability and effectiveness of the current accounting provision through a number of additional changes.

1. What are the current regulations?

The current rule at § 164.528 provides an individual the right to an accounting of disclosures of his or her protected health information. A disclosure is defined at § 160.103 as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information." An individual whose protected health information has been disclosed has the right to receive an accounting of such disclosures. This accounting does not include certain categories of disclosures, such as those for treatment, payment, or health care operations, based on an authorization, or to family, friends, and others involved in the individual's care (for a full list of the current exemptions from the accounting requirement, see § 164.528(a)(1)).

Additionally, §§ 164.308 and 164.312 of the Security Rule require covered entities to maintain and periodically review reports of who accesses electronic protected health information. Under current regulations, while covered entities are required to log access to individuals' electronic protected health information, covered entities do not have to provide the information from these access logs to individuals.

2. What are we proposing?

Under the proposed § 164.528, the section will be divided into an individual's right to receive an accounting of disclosures and a right to receive an access report. The access report would be limited to only electronic protected health information in a designated record set. For each time that electronic designated record set information is accessed, whether by a member of the covered entity's or business associate's workforce (a use) or by someone outside the organizations (a disclosure), an access report would include the date and time of the access, the identity of the person accessing the information, and, if available, a description of the information that was accessed and what actions were taken while in the system (*e.g.*, create, modify, view, print, *etc.*). The covered entity would be required to permit the individual to narrow the request for an access report to a specific time frame or person. Covered entities would be required to provide the access report in the electronic form and format requested by the individual, if readily producible, unless otherwise requested by the individual in such other form and format as agreed to by the parties.

The accounting of disclosures would provide additional information than what would be provided in an access report for certain categories of disclosures, providing the date of the disclosure, what information was disclosed, the recipient of the information, and the purpose for the disclosure—for example, law enforcement. This is largely the same information as is currently required for an accounting of disclosures, with minor modifications. The accounting of disclosures would continue to apply to both paper and electronic protected health information.

The requirements governing the accounting of disclosures would be modified in several ways. The current requirement to disclose six years of disclosures would be reduced to three years. Covered entities would no longer be required to provide the full accounting for certain categories of disclosures that are currently subject to the accounting requirement, such as disclosures that are required by law and for health oversight purposes (though limited information about such disclosures would be captured in the access report to the extent that they involve direct access to electronic designated record set information). The accounting requirement would be limited to disclosures of information about an individual in a designated record set, rather than disclosures of any protected health information. The proposal would reduce the time permitted for a covered entity to respond to a request for an accounting of disclosures from 60 days to 30 days. A covered entity still could use a one-time extension of 30 days. A covered entity also would be required to provide individuals with the option of limiting their request to a specific timeframe, type of disclosure, or recipient. Finally, covered entities would be required to provide the accounting in the form and format requested by the individual if readily producible, otherwise in a readable hard copy form or such other form and format as agreed to by the parties.

3. What would be the impact of changes to accounting of disclosures requirements?

We believe that the proposed changes will benefit individuals by reducing the amount of time it takes for them to receive an accounting of disclosures. While we propose to exclude a number of categories of disclosures from the accounting requirements, as discussed in the preamble we have proposed to exclude disclosures that we believe are of limited interest to individuals. Accordingly, we believe the more limited scope of the accounting provision will not significantly diminish the benefit of the accounting, since individuals will continue to have a right to receive a full accounting for the disclosures that are most likely to have an immediate impact on their interests, such as disclosures for law enforcement, judicial proceedings, or public health investigations.

Based on our contacts with covered entities we have learned that the process of tracking disclosures involves a considerable amount of effort because data in different systems must be linked manually regardless of whether the data are stored electronically or as hard copy. We expect that the proposed changes to the accounting of disclosures requirements—to reduce the time to track disclosures from six years to three and eliminating the requirement to account for a number of categories of disclosures—will reduce this burden on covered entities and their business associates. The responses to the RFI indicated that covered entities receive very few requests for accounting of disclosures. However, we have no information on the number of disclosures covered entities and their business associates make annually. Therefore, we are unable to estimate the reduced burden the proposed regulatory changes will generate. We are also unable to estimate the additional burdens, if any, of offering these accountings in a machine readable or other electronic format (unless the individual requests otherwise). We ask for public comments or information that will help us estimate these burdens.

We have limited information on how long it takes to respond to an accounting request under the current rule. The information that we have received has suggested that not more than 30 days is needed to respond to an accounting request under the current rule. Furthermore, our proposed rule will reduce the scope of information that is subject to an accounting. Accordingly, we believe there will be little burden on covered entities to respond to requests in 30 days, rather than 60 days. In circumstances where more than 30 days is needed, we continue to permit a single 30-day extension. We solicit public comment on this issue.

4. What would be the impact of adding the right to an access report?

We believe that the proposed right to an access report will provide a significant benefit to all individuals by providing them a means to learn who has accessed their electronic protected health information. This offers a significant benefit over the current accounting rule in that it provides individuals an opportunity to learn of access by members of the covered entity's workforce.

Almost all information required to satisfy a request for an access report is currently required under the Security Rule at §§ 164.308(a)(1)(ii)(D) and 164.312(b). We expect that the additional burden to covered entities will consist of, in response to a request, generating access reports for each electronic designated record set system and aggregating this information into a single electronic access report. The cost to covered entities to prepare an access report would be directly tied to the number of requests. Based on the experience covered entities have reported with requests for accountings of disclosures, we anticipate few requests for access reports. Therefore we expect the costs to generate access reports will be minimal. We request comment on the number of anticipated access reports, the burden of tracking access to electronic designated record set information, including whether our proposal will have any unintended effects by requiring significant changes to existing systems, and the burden caused by generating an access report.

The covered entity must produce within 30 days the access report in the electronic form and format requested by

the individual, if readily producible, unless the individual requests another mutually agreed upon format. We thus also request comment on the additional burden, if any, of providing electronic access reports (either in machine readable or other electronic format).

Some covered entities' systems may log a user ID but not a name, in which case there will be a burden on the covered entity to convert the identifier into a user name. The requirement to include in the access report information about users' actions while within the system and what information was accessed should create minimal burden since we only propose to require the inclusion of this information if it is available in the access logs.

The provision permitting individuals to limit their requests to a time period or person may limit the burden to produce an access report. Yet, modifying a standard report may require additional programming which would increase burden on the covered entity and business associates. We solicit comment on the effects of this provision.

5. What alternatives did we consider?

In light of the language of section 13405(c), we considered applying the access report requirements to only disclosures for treatment, payment, and health care operations through an EHR. We chose to expand the requirements for access reports to all electronic designated record set information because we believe that all such systems should be capable of logging access. We also believed that limiting the rule to EHR systems would lead to confusion among covered entities, business associates, and individuals regarding which systems were subject to the accounting provision. We chose to include uses, in addition to disclosures, because we believe that individuals have an interest in learning of access to their information by members of a covered entity's and business associate's workforces, and because it may be difficult for covered entities and business associates to distinguish between uses and disclosures through the use of automated systems.

We also considered requiring access reports to include the purpose of the disclosure. However, we believed the burden of collecting such information significantly outweighed the interests of most individuals in learning of such information, especially with respect to older EHR systems (where the burden of modifying systems may be highest). We will continue to reassess this option and to work with ONC to evaluate whether information about the purpose of disclosures should be part of future standards, such as standards governing electronic health information exchange.

C. How much will it cost covered entities to notify individuals of their new privacy rights?

Covered entities must provide individuals with notices of privacy practices that detail how the covered entity may use and disclose protected health information and individuals' rights with respect to their own health information. Beginning on January 1, 2013, individuals would have the right to receive a report of who accessed their electronic protected health information that covers a three-year period from the date of the request. Covered entities would have to revise their privacy notices to reflect this change.

The cost analysis for revising privacy notices is divided into an analysis of provider costs and an analysis of plan and insurer costs. For providers, given that the requirements described in this rule only require modification of one sentence in the notice of privacy practices, we estimate that drafting the updated notices will require approximately one-third of an hour of professional, legal time at approximately $90 per hour—or $30—that includes hourly wages of $60 plus 50 percent.[5] The total cost for attorneys for the approximately 669,000[6] health care providers in the U.S. is, therefore, expected to be approximately $20 million. Pursuant to § 164.520(c)(2)(iv), providers will be required to make the revised notice available upon request on or after the effective date of the revision. We anticipate publishing the final rule in late 2011 which should give providers enough time before the January 1, 2013, and 2014 compliance dates to exhaust current inventories of privacy notices and adequately manage the transition to revised notices. Therefore, we believe that this should not represent any additional burden, with respect to printing and distribution, above and beyond the existing requirements to distribute notices of privacy practices. Therefore, the total cost for providers is approximately $20 million. Because of the uncertainty surrounding the costs for revising privacy notices, we invite public comment on our analysis.

For health plans, we expect the cost of notifying policy holders to be minimal. Pursuant to § 164.520(c)(1)(i)(C), health plans must notify individuals within 60 days of a material change to its notice of privacy practices. Health plans will have until March 2, 2013, at the earliest (60 days after the January 1, 2013, compliance deadline), to notify members of the change to the privacy notice. We expect that this may be done in one of the health plans' annual mailings in order to minimize printing and distribution costs. Additionally, as indicated in Section IV.D., we are considering changes to the Privacy Rule's 60-day notification requirement for health plans, which may further reduce burden. Accordingly, we expect the only costs to be incurred would be for drafting the privacy policy notice revision. The costs should be similar to those for providers; that is, the cost of one third of an hour for an attorney to draft the revision. The cost we estimated would be $30 for each plan issuer notice. There may also be costs for plan issuers to post the changes on their web sites and to include language describing the changes and referring to the web site in their annual notices of plan changes. However, we believe the costs would be minimal.

With the exception of a few large health plans, most health plans do not self-administer their plans. The majority of plans are administered either by health insurance issuers (approximately 1,000) or by third party administrators that act on their behalf in the capacity as business associates. We identified approximately 3,500 third party administrators acting as business associates for approximately 446,400 ERISA plans identified by the Department of Labor. In addition, the Department of Labor identified 20,300 public non-Federal health plans that may use third party administrators. Almost all of the public and ERISA plans, we believe, employ third party administrators to administer their health plans. While the third party administrators will bear the direct costs of issuing the revised notices of privacy practices, the costs will generally be passed on to the plans that contract with them. Those plans that self-administer their own plans will also incur the costs of issuing the revised notices. We do not

[5] *http://www.bls.gov/oes/2008/may/oes231011.htm* for lawyers. The hourly rate + 50% is intended to account for fringes and overhead in addition to the standard hourly wages.

[6] We identified 673,324 entities that must prepare and deliver notices of privacy practices that are shown in Table 1 below. This includes 668,757 HIPAA covered entities that are health care providers, including hospitals, nursing facilities, doctor offices, outpatient care centers, medical diagnostic, imaging service, home health service and other ambulatory care service covered entities, medical equipment suppliers, and pharmacies. For the purposes of our calculation, we have rounded this number to 669,000. Table 1 also includes 4,567 health insurance carriers and third party administrators working on behalf of covered health plans. The cost estimates for these entities are addressed later.

know how many plans administer as well as sponsor health plans and invite comments on the number of self-administered plans; however, unless there were many such plans it would not have much effect on these estimates.

For the approximately 4,500 health insurance issuers and health plan administrators, we anticipate the cost of revising the change in the privacy policy notice to be approximately $135,000 (4,500 plans x $30 per draft revision). Although there may be costs associated with notifying enrollees of the change to the notice, we believe the cost should be minimal based on health plans including such notification in their annual plan update notices. We request public comment on our assumptions and analysis.

The total estimated cost for both providers and health plans to notify individuals and policy holders of changes in their privacy rights is approximately $20.2 million.

TABLE 1—NUMBER OF ENTITIES BY NAICS CODE [1]

NAICS	Providers/Suppliers	Entities
622	Hospitals (General Medical and Surgical, Psychiatric, Substance Abuse, Other Specialty)	4,060
623	Nursing Facilities (Nursing Care Facilities, Residential Mental Retardation Facilities, Residential Mental Health and Substance Abuse Facilities, Community Care Facilities for the Elderly, Continuing Care Retirement Communities).	34,400
6211–6213	Office of MDs, DOs, Mental Health Practitioners, Dentists, PT, OT, ST, Audiologists	419,286
6214	Outpatient Care Centers (Family Planning Centers, Outpatient Mental Health and Drug Abuse Centers, Other Outpatient Health Centers, HMO Medical Centers, Kidney Dialysis Centers, Free-standing Ambulatory Surgical and Emergency Centers, All Other Outpatient Care Centers).	13,962
6215	Medical Diagnostic, and Imaging Service Covered Entities	7,879
6216	Home Health Service Covered Entities	15,329
6219	Other Ambulatory Care Service Covered Entities (Ambulance and Other)	5,879
n/a	Durable Medical Equipment Suppliers [2]	107,567
4611	Pharmacies [3]	60,395
524114	Heath Insurance Carriers	1,045
524292	Third Party Administrators Working on Behalf of Covered Health Plans	3,522
Total Entities		673,324

[1] Office of Advocacy, Small Business Administration, *http://www.sba.gov/advo/research/data.html*.
[2] Centers for Medicare and Medicaid Service covered entities.
[3] The National Association of Chain Drug Stores.

D. Regulatory Flexibility Analysis

The Regulatory Flexibility Act requires agencies that issue a proposed rule to analyze and consider options for reducing regulatory burden if the regulation will impose a significant burden on a substantial number of small entities. The Act requires the head of the agency to either certify that the rule would not impose such a burden or perform a regulatory flexibility analysis and consider alternatives to lessen the burden.

The proposed rule would have an impact on covered health care providers, health insurance issuers, and third party administrators acting on behalf of health plans, which we estimate to be 673,324. Of the approximately $20.2 million in costs we are able to identify, the private sector will incur approximately 100 percent of the costs, or $20.2 million. The average cost per covered entity is therefore approximately $30. We do not view this as a significant burden. We note that the 3,500 third party administrators included in this calculation serve as business associates to the approximately 446,000 ERISA plans, most of which are small entities. We have no information on how many of these plans self-administer, and we request any data the public may provide on this question. Based on the relatively small cost per covered entity, the Secretary certifies that the proposed rule would not have a significant impact on a substantial number of small entities. However, because we are not certain of all the costs this rule may impose or the exact number of small health insurers or third party administrators, we welcome comments that may further inform our analysis.

VII. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), agencies are required to provide a 60-day notice in the Federal Register and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

a. Whether the information collection is necessary and useful to carry out the proper functions of the agency;

b. The accuracy of the agency's estimate of the information collection burden;

c. The quality, utility, and clarity of the information to be collected; and

d. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. We explicitly seek, and will consider, public comment on our assumptions as they relate to the PRA requirements summarized in this section. To comment on this collection of information or to obtain copies of the supporting statement and any related forms for the proposed paperwork collections referenced above, e-mail your comment or request, including your address and phone number, to *sherette.funncoleman@hhs.gov,* or call the Reports Clearance Office on (202) 690–6162. Written comments and recommendations for the proposed information collections must be directed to the OS Paperwork Clearance Officer at the above e-mail address within 60 days.

1. Abstract

Section 13405(c) of the HITECH Act requires the Secretary to promulgate regulations to require covered entities to account for disclosures to carry out treatment, payment, and health care operations through an EHR. In this

notice of proposed rulemaking, we propose to implement modifications that are partly required by section 13405(c) of the HITECH Act and partly based on our general authority under HIPAA by requiring covered entities to provide an individual with an access report upon request that includes information about each time that electronic protected health information in a designated record set is accessed. We also propose, based on our general authority under HIPAA, to modify the existing right to an accounting of disclosures to improve the effectiveness and workability of the provision. We seek public comment on our proposals.

We anticipate that the paperwork burdens on covered entities to comply with this proposed rule will include revising notices of privacy practices and providing accounting of disclosures and access reports to individuals upon request. The estimated annualized burden table below was developed using the same estimates and workload assumptions in the impact statement in the section regarding Executive Orders 12866 and 13563, above.

We propose to require covered entities and business associates to maintain the information necessary to generate accountings of disclosures and access reports for three years. With respect to accountings of disclosures, this is a shortening of the retention period and therefore should reduce their information collection burden. With respect to access reports, covered entities and business associates should already be collecting and retaining this information in accordance with their obligations under the Security Rule and their business associate agreements, and furthermore should be collecting and maintaining access logs as part of their usual and customary business.

2. Estimated Annualized Burden Hours

Section	Type of respondent	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
164.520	Revision of Notice of Privacy Practices for Protected Health Information.	673,324	1	30/60	336,662
Total					336,662

List of Subjects in 45 CFR Part 164

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Hospitals, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements, Security.

For the reasons set forth in the preamble, the Department proposes to amend 45 CFR Subtitle A, Subchapter C, part 164, as set forth below:

PART 164—SECURITY AND PRIVACY

1. The authority citation for part 164 is revised to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–9; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320–2(note)); and secs. 13400—13424, Pub. L. 111–5, 123 Stat. 258–279.

2. Amend § 164.520 to revise paragraph (b)(1)(iv)(E) as follows:

§ 164.520 Notice of privacy practices for protected health information.

* * * * *

(b) * * *

(iv) * * *

(E) The right to receive an accounting of disclosures of protected health information and an access report as provided by § 164.528; and

* * * * *

3. Revise § 164.528 to read as follows:

§ 164.528 Accounting of disclosures of protected health information and access report.

(a)(1) *Standard: Right to an accounting of disclosures of protected health information.* (i) Except as provided in paragraph (a)(1)(ii) of this section, an individual has the right to a written accounting of the following disclosures of protected health information about the individual in a designated record set by a covered entity or business associate made in the three years prior to the date on which the accounting is requested:

(A) Disclosures not permitted by this subpart, unless the individual has received notification of the impermissible disclosure pursuant to § 164.404;

(B) For public health activities as provided in § 164.512(b), except disclosures to report child abuse or neglect pursuant to § 164.512(b)(1)(ii);

(C) For judicial and administrative proceedings as provided in § 164.512(e);

(D) For law enforcement purposes as provided in § 164.512(f);

(E) To avert a serious threat to health or safety as provided in § 164.512(j);

(F) For military and veterans activities, the Department of State's medical suitability determinations, and government programs providing public benefits as provided in § 164.512(k)(1), (4), and (6); and

(G) For workers' compensation as provided in § 164.512(l).

(ii) A covered entity need not account for a disclosure under paragraph (a)(1)(i) of this section if it also is required by law, unless such disclosure falls under paragraphs (a)(1)(i)(C) or (D).

(2) *Implementation specification: Content of the accounting.* (i) The accounting must include for each disclosure:

(A)(*1*) The date, if known; or if not, the approximate date or period of time during which the disclosure occurred which, at a minimum, shall 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; or

(*2*) For multiple disclosures to the same recipient for a single purpose, the dates, as described in paragraph (a)(2)(i)(A)(*1*) of this section, of the first disclosure and the last disclosure in the accounting period.

(B) The name of the entity or natural person who received the protected health information and, if known, the address of such entity or person, except when such information constitutes protected health information about another individual, in which case a description such as "another patient," "another enrollee," or similar language must be included;

(C) A brief description of the type of protected health information disclosed; and

(D) A brief description of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such description, a copy of a written request for a disclosure under § 164.512, if any.

(ii) The covered entity shall provide the individual with the option to limit the accounting of disclosures to a specific time period, type of disclosure, or recipient.

(3) *Implementation specification: Provision of the accounting.* (i) The covered entity must act on the individual's request for an accounting no later than 30 days after receipt of such a request, as follows.

(A) The covered entity must provide the individual with the accounting requested; or

(B) If the covered entity is unable to provide the accounting within the time required by paragraph (a)(3)(i) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(*1*) The covered entity, within the time limit set by paragraph (a)(3)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(*2*) The covered entity may have only one such extension of time for action on a request for an accounting.

(ii) The covered entity must provide the accounting in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(iii)(A) The covered entity must provide the first accounting to an individual in any 12-month period without charge and inform the individual at the time of the request that there may be a fee for each subsequent request for an accounting by the individual within the 12-month period.

(B) The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that the covered entity informs the individual of the fee at the time of the subsequent request and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(iv) The covered entity may require individuals to make requests for an accounting in writing provided that it informs individuals of such a requirement.

(4) *Implementation specification: Law enforcement delay.* (i) If a law enforcement official states to a covered entity that providing an accounting to an individual of disclosures to the law enforcement official would be reasonably likely to impede the law enforcement agency's activities, the covered entity shall:

(A) If the statement is in writing and specifies the time for which a delay is required, delay providing the individual with an accounting of disclosures for such purposes for the time period specified; or

(B) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay providing the individual with an accounting of disclosures for such purposes temporarily and no longer than 30 days from the date of the oral statement unless a written statement as described in paragraph (a)(4)(i)(A) of this section is received during that time.

(ii) The covered entity shall account for all other disclosures in accordance with paragraph (a) of this section and shall supplement the accounting with information about the disclosures to law enforcement upon expiration of the requested law enforcement delay.

(5) *Implementation specification: Documentation.* (i) Notwithstanding § 164.530(j)(2), for each disclosure that is subject to the accounting requirements of this section, a covered entity or business associate must retain the information required to be included in an accounting under this section for three years from the date of the disclosure.

(ii) A covered entity must document the following and retain the documentation as required by § 164.530(j):

(A) A copy of the written accounting that is provided to the individual under this section; and

(B) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

(b)(1) *Standard: Right to an access report.* An individual has a right to receive a written access report that indicates who has accessed protected health information about the individual in an electronic designated record set maintained by a covered entity or business associate for up to three years prior to the date on which the access report is requested.

(2) *Implementation specification: Content of the access report.* (i) The covered entity must provide the individual with an access report that includes the following:

(A) Date of access;

(B) Time of access;

(C) Name of natural person, if available, otherwise name of entity accessing the electronic designated record set;

(D) Description of what information was accessed, if available; and

(E) Description of action by the user, if available, e.g., "create," "modify," "access," or "delete."

(ii) The covered entity shall provide the individual with the option to limit the access report to a specific date, time period, or person. The covered entity may provide the individual with the option to limit the access report to a specific organization, such as the covered entity or a specific business associate.

(iii) The covered entity must provide the access report in a format that is understandable to the individual.

(3) *Implementation specification: Provision of the access report.*

(i) The covered entity must act on the individual's request for an access report no later than 30 days after receipt of such a request, as follows.

(A) The covered entity must provide the individual with the access report requested; or

(B) If the covered entity is unable to provide the access report within the time required by paragraph (b)(3)(i) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(*1*) The covered entity, within the time limit set by paragraph (b)(3)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the access report; and

(*2*) The covered entity may have only one such extension of time for action on a request for an access report.

(ii) The covered entity must provide the individual with the access report in a machine readable or other electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. If the individual requests the access report in hard copy form, the covered entity must provide the individual with the access report in a readable hard copy form. For purposes of this paragraph, machine readable data is digital information stored in a standard format enabling the information to be processed and analyzed by computer.

(iii)(A) The covered entity must provide the first access report to an individual in any 12-month period without charge and inform the individual at the time of the request that there may be a fee for each subsequent request for an access report by the individual within the 12-month period.

(B) The covered entity may impose a reasonable, cost-based fee for each subsequent request for an access report by the same individual within the 12-month period, provided that the covered entity informs the individual of the fee at the time of the subsequent request and provides the individual with an opportunity to withdraw or modify the request for a subsequent access report in order to avoid or reduce the fee.

(iv) The covered entity may require individuals to make requests for an access report in writing provided that it informs individuals of such a requirement.

(4) *Implementation specification: Documentation.* (i) Notwithstanding § 164.530(j)(2), for each use or disclosure that is subject to the access report requirements of this section, a covered entity or business associate must retain the information required to be included in an access report under this section for three years from the date of the use or disclosure.

(ii) A covered entity must document the following and retain the documentation as required by § 164.530(j):

(A) A copy of the access report that is provided to the individual under this section; and

(B) The titles of the persons or offices responsible for receiving and processing requests for an access report by individuals.

(c) *Confidentiality of patient safety work product.* A covered entity shall exclude from an accounting or access report under this section any information that meets the definition of *patient safety work product* at 42 CFR 3.20.

Dated: February 7, 2011.

Kathleen Sebelius,

Secretary.

[FR Doc. 2011–13297 Filed 5–27–11; 8:45 am]

BILLING CODE 4153–01–P