KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

August 1, 2011

Georgina Verdugo
Director, Office of Civil Rights
United States Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F, HHH Bldg.
Washington, D.C. 20201

Re: RIN: 0991-AB62

Dear Ms. Verdugo:

The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive, workable privacy and security policies to protect health data as it is exchanged using information technology. CDT is frequently relied on for sound policy advice regarding the challenges to health privacy and security presented by health information technology (health IT) initiatives. We have testified before Congress four times on the privacy and security issues raised by health IT, and we chair the privacy and security working group of the federal Health IT Policy Committee (called the "Tiger Team"). CDT submits these comments, endorsed by the signatories below, in response to the to the Office of Civil Rights' (OCR) May 31, 2011 Notice of Proposed Rulemaking (NPRM) on the *HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act* (HITECH).[1]

I. Introduction

CDT has repeatedly called for a comprehensive framework of privacy and security protections for health data that address the full complement of fair information practices (FIPs).[2] FIPs, which provided the foundation for the HIPAA Privacy and Security Rules, are fundamental to privacy law both domestically and internationally. The Office of the National Coordinator for Health Information Technology (ONC) also adopted FIPs through the

[1] 76 Fed. Reg. 31426 – 31449 (May 31, 20110).
[2] See, for example, McGraw D., Dempsey JX, Harris L, Goldman, J. Privacy as Enabler, not an impediment: Building trust into health information exchange. Health Affairs 2009; 28(2): 416-27.

Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.[3]

Openness and transparency about personal information access, use and disclosure is a fundamental tenet of FIPs. Transparency supports accountability, consumer choice and trust while providing a deterrent to unauthorized access. A recent survey by the Markle Foundation indicates that both doctors and the public strongly support letting patients see who has accessed their records,[4] and requirements to account for disclosures provide a vehicle for greater transparency into how an individual's information is actually accessed, used and disclosed.

True transparency should apply throughout the data lifecycle, from the notice of privacy practices a patient receives in a medical office or upon signing up for a health plan to enabling patients to learn how their health information is accessed and used – and the advent of health information technology (health IT) and automated tracking makes this vision more possible.

The Fair Credit Reporting Act (FCRA) provides an example of how to provide greater transparency to individuals about access to personal information about them. Under FCRA, credit reporting agencies are required to provide individuals, upon request, with a report of who has accessed their credit report and when this access occurred.[5] This was the model of transparency envisioned by CDT and others who advocated before Congress for an expansion of transparency rights under HIPAA, particularly for providers using electronic health records (EHRs).

In HITECH, Congress laid the groundwork for realizing this vision by expanding the scope of disclosures required to be accounted for under the HIPAA Privacy Rule.[6] However, Congress also recognized the critical role that technology would need to play in realizing the potential for greater transparency of disclosures of health information. For example, Congress limited the expansion of this right only to covered entities adopting an EHR. Congress also required HHS to adopt a technical standard to enable EHRs to track such expanded disclosures automatically. But Congress also recognized that fulfilling the vision of greater transparency would require a delicate balancing of the interests of patients and the potential burdens on covered entities. In this proposed rule, OCR tries admirably to strike this balance through the creation of the new "access report" requirement.

---

[3] Dept. of Health and Human Services, Office of the National Coordinator, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, Dec. 15, 2008, pg. 7, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf.

[4] Seventy-three percent of doctors and 79 percent of patients agreed on the importance of a policy that individual patients be able to review who has had access to their personal health information. Markle Foundation, "The Public and Doctors Overwhelmingly Agree on Health IT Priorities to Improve Patient Care," January 31, 2011, Pg. 6, http://www.markle.org/publications/1461-public-and-doctors-overwhelmingly-agree-health-it-priorities-improve-patient-care.

[5] 15 U.S.C. 1681g(a).

[6] HITECH Sec. 13405(c)(4)(B).

CDT was one of the drafters of and a signatory to comments submitted in response to OCR's Accounting of Disclosure Request for Information (RFI) by the Consumer Partnership on eHealth, a non-partisan coalition of patient and consumer organizations. In these comments, we urged OCR to utilize the audit trail used by EHRs in order to at least initially fulfill the mandate from Congress.[7] We acknowledged that an audit trail would encompass both access and disclosure of information from a record. Since we were aware that audit trails typically do not distinguish between access and disclosures under HIPAA, we erred on the side of providing patients with greater transparency, and assumed this would be easier for entities to accomplish using existing automated functionalities. We also urged HHS to initially implement a more rudimentary accounting of disclosures expansion, and then to work long-term to phase in requirements that provide patients with even greater transparency in the future – such as a requirement that the accounting include the recipient of data disclosed from a health record and the purpose of such disclosures – when critical technical functionalities to meet those objectives could be developed and included in standard EHR technology.

We greatly appreciate the responsiveness of OCR in this proposed rule to our suggestions. In its NPRM, OCR did largely craft rules based on the information OCR believed covered entities already captured automatically through EHR audit trail capabilities and Security Rule compliance.[8] However, developments that have occurred since the release of the RFI and some concerns expressed by covered entities call into question our assumptions about the technical capabilities of EHRs that were the basis of our recommendations in the RFI.[9] As set forth in more detail below, we now share the concerns expressed by many that the proposed access report is not implementable as currently proposed.

We recommend that, after the close of this initial comment period, OCR engage in further dialogue with consumer groups and industry stakeholders, including technology vendors, focused on implementation of an interim solution for the access report that takes steps toward increasing transparency of record access and leverages existing technical capabilities. We also urge OCR to consider this a first step in the process and to work with ONC over the long-term to provide incentives for EHRs to adopt capabilities to provide greater transparency about health record access, use and disclosure in the future. CDT is committed to actively participating in a multi-stakeholder process to resolve these concerns. The time to begin building comprehensive effective accounting and access capabilities into systems that handle e-PHI is now, as health IT is still taking off and the ground rules are still being established.

---

[7] National Partnership for Women and Families, Comments of the Consumer Partnership for e-Health to *Request for Information on HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act*, May 18, 2010, Pgs. 6-7, http://www.nationalpartnership.org/site/DocServer/OCR__HHS_____Accounting_of_Disclosures_ __CPeH___2010-May.pdf?docID=7664.

[8] 76 Fed. Reg. 31437.

[9] OCR acknowledged the controversy of the Accounting of Disclosure provisions in the preamble to the Proposed Rule. 76 Fed. Reg. 31427-31428.

Our comments are set forth in detail below. In summary:

- With respect to the new access report, we propose that OCR focus in the short term (over the next year) on requiring covered entities and business associates to provide patients, upon request, with a copy of the audit trail they are currently using (if they are using one for security purposes or to meet the requirements of the HIPAA Security Rule). With respect to this initial, short-term solution, we also recommend OCR:
    - Apply the access report to relevant portions of the EHR;
    - Delete the requirement that the access report include the names of individuals accessing a patient's record;
    - When relevant, allow entities to satisfy access report requests with an internal "privacy investigation;" and
    - Require covered entities to produce the access reports of business associates who can generate them (accompanied by a list of names of any business associates who cannot).
- We recommend that OCR work over the long-term (over the next 2-3 years) with ONC to provide incentives for technology to produce an access report that is more meaningful for patients.
- With respect to the proposed Accounting of Disclosure provisions, we recommend OCR:
    - Require accounting of public health disclosures required by law, particularly when they relate to a specific individual (vs. those that are population-based);
    - Require accounting of disclosures to or through a health information exchange (HIE) that serves as a data repository, particularly in circumstances where patients have not been provided with a choice regarding whether or not to participate.
    - Require accounting in circumstances where breach notification to an individual may not have occurred.
- With respect to the proposed new accounting provisions, we support extending coverage to information in a designated record set, as well as the time for response, the time period to be covered by the accounting, and the requirement to include the data recipient. We also counsel OCR to develop measures to provide greater transparency to patients regarding research potentially using their health information.
- We also agree with the need to provide notice of these changes in a revised notice of privacy practices.

II. Develop interim "access report" that works in the short-term; phase in a more comprehensive solution over time

A. Concerns about technical feasibility of proposed access report

As noted above, in comments submitted by CPeH, CDT urged OCR to rely on current audit trail functionalities presumed to be in EHRs to provide individuals with a

mechanism for learning who has accessed their record. However, our assumptions about the capability of audit trails appear to have been too optimistic. Specifically:

- Our assumptions about the data typically collected in an audit trail were largely based on the certification requirements for audit trail functionalities in Certified EHR Technology for Stage 1 of the Meaningful Use Incentive Program. We assumed the certification requirements were based on commonly adopted industry standards, but we have since learned that the audit trail functionality in some EHR systems may not operate in ways that are conducive to providing an access report to patients.[10] In addition, to the extent that the Security Rule requires entities to be able to track and monitor health record access, there is some flexibility with respect to how this requirement is implemented that is not necessarily reflected in the proposed access report.

- In addition, covered entities are not required by the HIPAA Security Rule to merge audit logs from multiple systems, normalize the data, and generate a single human-understandable "report." A requirement to generate a human-intelligible access report that spans multiple systems arguably is a new requirement that will require retrofitting of systems or additional resources to implement. We greatly appreciate the effort to make audit trail reports more digestible by, and relevant to, individuals – but the requirement to produce a single, readable access report (potentially across multiple systems) is beyond what can be easily (and cost effectively) done using current technology.

- In addition, business associates are required by HITECH to comply with the Security Rule – but the details of that requirement are still being worked out in regulation and are not yet enforceable. As a result, business associates also are not required to have (and may not yet have) audit trail functionality for their record systems.

- With respect to the requirement to establish an accounting of disclosure standard for EHRs, HHS proposed one for EHR certification for the first stage of the meaningful use incentive program – but the standard was made optional in response to concerns from vendors that it was not specific enough and could not be implemented in time for the meaningful use program to begin in 2011. The standard remains optional for Certified EHR Technology, and the extent to which this standard is incorporated in the technology is not known.

- In the CPeH comments, we noted that many individuals asking for an accounting of disclosures would likely do so in response to suspicion of inappropriate access to their records. CDT has subsequently seen an example of what a likely access report from a single institution would look like (over just a one month period), and

[10] See, e.g., College of Healthcare Information Management Executives, Comments to *Notice of Proposed Rulemaking to HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act*, July 21, 2011, Pg. 4, http://www.cio-chime.org/advocacy/resources/download/CHIME_Comments_OCR_NRPM_for_HIPAA_Changes.pdf.

the volume of information would be nearly impossible for an individual to sort through to determine inappropriate access.

- OCR's clarification that covered entities and business associates need only provide a report of access to a designated record set was clearly intended to limit the scope of the access report. Although the NPRM describes this proposal as "*limiting* the accounting provision to PHI in a designated record set,"[11] some stakeholders believe that the designated record set could be considerably broader than what was intended in HITECH.

We are optimistic that a number of the issues identified above can be worked through – but not in the time period allowed prior to the close of the comment period. We ask OCR to continue to actively engage consumer groups and covered entities after the close of the comment period in an effort to find both short and long-term solutions that provide greater transparency for individuals, while leveraging technology to minimize the burden of both collecting and reporting information on record access and disclosures to patients. Realistically, the short-term solution will likely need to be a stop-gap measure based on what is achievable over the next two years while technology is developed to more specifically address transparency for individuals in ways that more resemble the right provided under the FCRA – for example, focusing more on reporting of disclosures rather than all access, including at least broad categories of purpose for a disclosure, and including the entity that was the recipient of the information.

B. Short-term issues for resolution

In order to take concrete steps toward achieving the type of transparency provided to consumers by the FCRA, we suggest that OCR focus on the following:

1. Clarify scope of what is covered by access report

As noted above, covered entities and business associates are concerned that the requirement to provide a report on access to PHI in a "designated record set" could be interpreted to extend to information in electronic systems that are not technically part of the core "electronic health record" system intended by Congress in HITECH. CDT supports clarifying the scope of the access report so that it more clearly targets information in an "electronic health record." We do not have a commonly accepted definition of an EHR, and we are not suggesting that the access report requirement apply only to users of Certified EHR Technology. Rather, the certification requirements can perhaps help scope out some parameters of what should be covered by the access report. At a minimum, the scope of information required to be included in an access report should not extend to systems that are not likely to be monitored using audit logs.

2. Name of individual who has accessed a patient's data

OCR proposes to require that the access report contain the full name of recipients accessing patients' health records, where available.[12] However, the NPRM cites covered

[11] 76 Fed. Reg. 31430.
[12] 76 Fed. Reg. 31438.

entities' concerns over the safety and privacy of their workforce members in this requirement.[13] Some covered entities have expressed concerns that disgruntled patients or malicious actors could misuse a list of a covered entity's employees.

CDT is skeptical that an individual provider or employee has a legitimate privacy interest in how she accesses health records in her professional capacity, particularly in a highly regulated industry such as health care. However, CDT is also unconvinced that the employee's name is especially useful to patients seeking an access report. An employee's name alone tells a patient very little regarding why her PHI was accessed. FCRA does not require credit agencies to release the names of particular individuals who have accessed a credit report; instead, the report needs to include the identity of the organization or entity accessing the report.

Rather than include the employee's name, a better approach may be to include the department or unit in which the employee was working at the time she accessed the patient's PHI (or her role within the organization), if such information is captured by the audit trail. If the recipient is not an employee of the covered entity, the organization of the recipient should be included (which is permitted by the NPRM). Including the department or unit could also suggest the reasons why the patient's information was accessed, which is information likely to be of more interest to the patient.

3. Where relevant, allow entities to satisfy access report requests with an internal "privacy investigation"

As we noted in the comments to the RFI submitted by CPeH, a primary reason why individuals might ask for an access report is to check on inappropriate access to his or her medical records. In such cases, the entity should be permitted to work with the patient to determine if an access report is needed or if instead the entity should resolve the individual's concerns through an investigation of the suspected inappropriate access. The proposed rule already includes provisions that allow covered entities to suggest narrowing the scope of the request, presumably down to a single individual.[14] These provisions could be clarified to make it more clear that the entity can resolve an individual's request for an access report by promptly and thoroughly investigating the patient's particular concern (within the same timeframes – or shorter – as the access report), as long as limiting the request in this way is agreeable to the patient.

4. Give patients the right to see (and obtain a copy of) what is currently generated in audit logs, without a requirement to combine them into one, human understandable report

Providing transparency to individuals about access to their records ideally should mean the provision of a single report, that spans all of the electronic medical record systems that make up an entity's EHR, and that is human readable and understandable without additional assistance from the covered entity. We applaud OCR for bringing a strongly patient-centered approach to the proposed rule.

[13] 76 Fed. Reg. 31428.
[14] 76 Fed. Reg. 31439.

However, given the concerns about technical capability raised in these comments and those submitted by others, we propose that an interim, short-term solution, developed over the next 6 months to a year, would be to require providers to give the patient, upon request, a copy of the audit trail as currently generated by its EHR, without a requirement to merge multiple reports into one or to make it understandable on its own, without further intervention from the entity.[15] Such an approach would leverage current technology to take the first steps toward achieving greater transparency for patients without imposing additional burdens on entities. To some extent the NPRM reflects this approach. For example, it requires access reports to list a description of the information accessed if this information is available.[16] Other desired elements of the access report could be made subject to technical and resource availability. Another advantage to this approach is that it more closely reflects the flexibility of the current Security Rule – a requirement to give patients, upon request, a view or copy of what is currently collected can arguably be done by both small and large entities.

We recognize that this will not provide as much value to individuals; hence, it is critical that this be considered a very short-term, first-step solution in order to provide more time to consider how EHR technology can evolve to automatically generate reports that focus on information more likely to be of value to individuals. We believe that requests for such reports will continue to be relatively rare (particularly if entities develop sound processes for investigating particular complaints of record access in lieu of issuing a report); consequently, we are erring on the side of leveraging currently technology for these reports to avoid placing significant burdens on entities to create technical capacity to respond to requests that likely will rarely come.

We have also heard concerns of industry that individuals will be "unduly alarmed" by a report of access to their record. We believe that promoting openness and transparency about the sharing of personal health information is critical to building trust in health IT systems. The need to build such trust would be undermined by a "black box" approach to record sharing. Health care providers should engage in a dialogue with their patients to explain the legitimate purposes for accessing records and the steps the provider takes to prevent unauthorized access.

5. Business associate access requirements

The NPRM proposes to require the access report to include any access to electronic PHI held in a designated record set by covered entities or business associates. HITECH required covered entities to provide either an accounting that includes disclosures by business associates or an accounting of its own disclosures and a list of business associates and their contact information.[17] The NPRM would eliminate the second option, requiring the covered entities' access reports to include uses and disclosures by business associates, rather than provide a list of business associates.[18]

---

[15] Entities that collect audit trails with employee names should be given the flexibility to remove employee names from the reports or leave the names in the reports, depending upon provider policies and the specific needs of the patient making the request.
[16] 76 Fed. Reg. 31438.
[17] Sec. 13405(c)(3).
[18] 76 Fed. Reg. 31437.

CDT supports the NPRM's elimination of the list option for business associate access. The list option would merely shift the burden of compiling access and disclosure records from the covered entity to the patient, when it is the covered entity – and rarely the patient – that has the direct relationship with the business associates. CDT urges OCR to keep the proposed language that eliminates the list option and requires covered entities to account for the disclosures of its business associates.

However, as mentioned above, business associates are not yet held accountable by OCR for complying with the HIPAA Security Rule. Consequently, the requirement to generate an audit trail upon request should apply to all business associates currently using them and be phased in for all business associates on the same schedule as the rules for compliance with the security rule are phased in. In the short-term, patients requesting an access report can be provided with a list of those business associates who do not use audit trail technology and therefore cannot produce access reports.

6. Deadline for producing an access report

As a final note, we support the requirement of 30 days (with the possibility of just one 30-day extension, with explanation provided to the patient as to why) to produce an access report. We note that this deadline will be even easier to meet if the above recommendations are followed.

C. Long-term work to achieve more effective openness and transparency

As discussed extensively in these comments, the limitations of current EHR technology provide us with few options for achieving greater transparency for record access and disclosure for patients in a way that is automated and minimizes the burden on covered entities and business associates. Ideally, such transparency would focus more on sharing of data external to a system, which identifies the organization or entity who has received the information, the purpose for which it was shared, the date it was shared and the type of information shared (if not the actual data elements shared) – all in format that is easily understandable for patients. It may even be more desirable to have one report of disclosures, versus separate reports of access and an accounting of disclosures. Achieving this type of FCRA-like transparency does not appear to be possible using current technology, and it is unlikely the market alone will generate sufficient incentives to drive the necessary innovation.

OCR should work closely with ONC over the long-term to more comprehensively address these issues. The short-term solution we recommend exploring above will be rudimentary and far from ideal for either patients or covered entities and business associates. We urge OCR to use this opportunity to launch a more forward-looking commitment to working with ONC to promote greater health record sharing transparency in order to continue to build public trust in health IT systems. OCR and ONC should ideally engage multiple stakeholders, including providers, consumer and patient groups, and health IT experts and vendors, in order to work toward policies and technical standards that promote greater openness and transparency in an implementable fashion. This long-term solution should be developed in time to be deployed in Stage 2

or 3 of the EHR certification program, in order to leverage the financial incentives of HITECH.

III. Accounting for Disclosures

A. Public Health Disclosures

CDT believes patients want to know when their information is disclosed for public health purposes, and CDT agrees with OCR that the accounting report should include public health disclosures.[19] However, in order to strike the right balance between a patient's right to an accounting and the need to protect public health, CDT believes some aspects of the proposed rule need clarification or redefinition.

The NPRM proposes to exempt disclosures required by law from the accounting of disclosures.[20] However, the exemption may weaken the requirement that the accounting include disclosures for public health, because numerous disclosures for public health are required by law. CDT urges OCR to exclude public health disclosures from the exemption for disclosures required by law. At a minimum, OCR should require that disclosures required by law that relate to a specific individual and that contain individually-identifiable information – rather than those that are population-based and stripped of patient identifiers – be included in the accounting.

Some public health disclosures are precisely the type that patients ought to know about, such as workforce surveillance examinations in which employees are often unaware that relevant health information is forwarded to their employers.[21] Without an accounting, some employees may never find out when their information is disclosed to their employer, and employees would have no mechanism to determine whether the right information is being passed along. Although having to account for these disclosures might add some administrative burden, the close relationship that medical surveillance and workforce injury providers typically have with employers can be leveraged to significantly reduce that burden.

B. TPO Exception for HIE

The NPRM would exclude disclosures for treatment, payment, and health care operations (TPO) from the accounting when they are made through a health information exchange (HIE).[22] CDT believes that the exception, as described, is too broad. OCR appears to have only considered TPO disclosures as they might occur when the HIE acts as a conduit between two separate EHR systems.[23] However, such disclosures could also occur in the HIE's capacity as a data repository. OCR also does not factor in whether patients have a choice in participating in the HIE.

---

[19] 76 Fed. Reg. 31431.
[20] 76 Fed. Reg. 31433.
[21] 45 CFR 164.512(b)(1)(v)(C).
[22] 76 Fed. Reg. 31440-31441.
[23] 76 Fed. Reg. 31440.

The accounting should include disclosures to an HIE acting as a repository of data and where patients have no opt in or opt out choice as to whether their PHI is shared with the HIE. Under the principle that the patient should not be surprised about what happens to their information, when the patient has no choice about whether or not their data is shared through one of these new arrangements, it should be included in an accounting requested by a patient.

C. Breach Notification

We applaud OCR for clarifying that the accounting of disclosures covers impermissible disclosures that do not qualify as a "breach" under current regulations.[24] Requiring the accounting of disclosures to include impermissible disclosures that don't meet this "harm standard" takes a step toward making patients aware of breaches for which they would otherwise not receive notification. To strengthen the accounting requirement further, OCR should require the accounting to include impermissible disclosures that do qualify as a "breach" under the current definition when the covered entity has insufficient or out-of-date contact information for the patient whose PHI had been breached. The substitute notice outlined in 45 CFR 164.404(d)(2) is less likely to reach patients for whom the covered entity does not have adequate contact information. Although including the impermissible disclosure in the accounting should not fulfill the substitute notice requirement, the accounting should nonetheless be used as an additional means to alert victims of breach whom the covered entity might have trouble contacting.

As CDT has stated previously, the current definition of "breach" – with its caveat that the breach pose a significant risk of financial, reputational or other harm to the individual – gives too much discretion to covered entities and business associates with regard to determining whether patients should know that their sensitive health information had been acquired, accessed or used by an unauthorized party.[25] CDT urges OCR to revise the current breach notification rule to eliminate the "*notify if* there is a significant risk of harm" formulation, and instead replace it with a "*notify unless* there is no significant risk of harm" formulation that requires covered entities to conduct and document a risk assessment in order to determine whether there is a significant risk.[26] OCR should not consider the accounting of disclosures to be an adequate replacement for a strengthened breach notification rule because of the infrequency with which patients currently make use of their right to an accounting and the low likelihood that many patients will use the accounting to search for breaches of health information for which they have not received notification.

---

[24] 45 CFR 164.402(1).

[25] See Joint Comments of the Center for Democracy & Technology and the Markle Foundation to the Dept. of Health and Human Services Interim Final Rule on Breach Notification for Unsecured Protected Health Information, October 23, 2009, http://cdt.org/files/pdfs/CDT%20Joint%20Comments_Areas%20of%20Concern_0.pdf.

[26] For an example of the "notify unless" formulation, see the White House Cybersecurity Proposal, Data Breach Notification, Sec. 101(a), May 12, 2011, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Data-Breach-Notification.pdf.

D. Disclosures for Research

We understand OCR's rationale for exempting research disclosures from the proposed new accounting of disclosure requirements. We also hear the arguments in favor of not requiring individuals to be provided with a copy of research protocols that might – or might not – include their health information. However, we urge OCR and other agencies within HHS to work toward a solution to provide greater transparency to the public regarding how data is used in research, for what purposes, and for what resulting public benefit. HHS' health reform and health IT initiatives are aimed at creating a learning health care system that performs better at a more reasonable cost, which is going to increase the demands for research using health data. If authorization is not going to be required for this type of research in all circumstances, we will need to have a solution that offers greater openness and transparency to the public about research as a potential "proxy" for authorization.

E. Limit to Designated Record Set

HIPAA currently provides a right to an accounting of disclosures of paper and electronic PHI regardless of whether it is in a designated record set.[27] HITECH addressed accounting of disclosures through an EHR, but not paper records.[28] The NPRM applies the accounting requirement to both paper and electronic PHI in designated record sets. In the NPRM, OCR requested comment on limiting the accounting requirement to PHI in a designated record set.[29] CDT supports applying the accounting requirements on designated record set data. We agree with OCR that individuals are most interested in health information used to make treatment and payment decisions about the individual, and not all of this information may be accessed or disclosed through an EHR.

F. Thirty-Day Response Time and Extension

CDT applauds OCR's decision to reduce the response time for requests for an accounting.[30] We agree with OCR's reasoning that the amount of time needed to respond to a request for an access report or an accounting of disclosures that go back three years – instead of six – reduces the need for a 60-day timeframe.[31] CDT supports providing covered entities with a singe 30-day extension, and also supports the requirement that covered entities provide a written statement to patients explaining any delay.[32]

[27] 45 CFR 164.528.
[28] Sec. 13405(c).
[29] 76 Fed. Reg. 31430.
[30] 76 Fed. Reg. 31435.
[31] 76 Fed. Reg. 31435.
[32] 76 Fed. Reg. 31440.

G. Time Period & Inclusion of Data Recipient

HIPAA requires covered entities and business associates to account for the previous six years, but HITECH gives individuals the right to receive an accounting of TPO disclosures from EHRs for the previous three years.[33] In its NPRM, OCR proposed to reduce the timeframe for accounting for disclosures to three years, and requested comment on specific concerns regarding the need for accounting of disclosures beyond three years.[34] CDT supports the three-year timeframe to reduce administrative burden and maintain consistency with HITECH.[35] CDT agrees with OCR that individuals are most likely to be interested in accesses and disclosures that occurred relatively recently. CDT also supports OCR's proposal to require the data recipient (at least organizational recipient) to be included in the accounting.

IV. Notice of Privacy Practices Revision

CDT supports the requirement that covered entities revise their notice of privacy practices as a material change to covered entities' privacy practices. CDT also supports OCR's proposal that covered entities be permitted to update their notices during their next annual mailing in order to reduce administrative burden.[36] The notices are not read or well understood by the majority of patients, and the present notice system is in serious need of reform in order to be effective. For now, however, the notice of privacy practices is the most viable vehicle for educating patients about their rights to an accounting of disclosures and an access report. OCR should continue to work with ONC and covered entities to improve patient engagement and education on privacy issues and patients' rights under HIPAA.

V. Conclusion

CDT remains fully committed to accounting of disclosures concept as a fundamental element of transparency. OCR has taken bold steps to establish the transparency and accountability patients want and that technology makes possible. OCR should focus over the next 6 months to a year on what current technology can accomplish and implement a long-term plan to leverage EHR certification to transform the accounting and access report requirements into a comprehensive system of transparency and accountability that matches consumer and business needs.

[33] Sec. 13405(c)(1)(B).
[34] 76 Fed. Reg. 31430, 31440.
[35] Sec. 13405(c)(1)(B).
[36] 76 Fed. Reg. 31441.

We thank OCR for this opportunity to submit comments. Please do not hesitate to contact us if we can be of any assistance.

Deven McGraw
Director, Health Privacy Project
CDT

Harley Geiger
Policy Counsel
CDT

These comments are submitted by the Center for Democracy & Technology and supported by the following organizations:

AARP
Caring From A Distance
Center for Medical Consumers
Childbirth Connection
Consumers Union of United States
Healthwise
Medical Advocacy Mural Project
National Consumers League
National Partnership for Women and Families
UHCAN Ohio