KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

October 26, 2011

Secretary Kathleen Sebelius
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, D.C. 20201

Re: HHS-OPHS-2011-0005

Dear Secretary Sebelius:

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 in response to HHS' July 26, 2011 Advance Notice of Proposed Rulemaking (ANPRM) on *Human Subjects Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay and Ambiguity for Investigators*.[1] As a result of our leadership of the Tiger Team, we played a major and influential role in shaping and subsequently writing the recommendations of the Tiger Team and Policy Committee on this ANPRM, which will also be submitted to HHS. This letter serves to offer our endorsement of the recommendations made in that letter, to reinforce a number of its points, and to submit our own recommendations in several areas not addressed by the Policy Committee. These areas include the treatment of identifiable and de-identified data; extending the scope of the Common Rule; and the proposal to harmonize HIPAA and the Common Rule where such consistency would be beneficial.

## I. Introduction

CDT supports the intent of the ANPRM to update key federal privacy regulations to respond to a changed health information environment. The success of a number of the emerging structures and programs associated with the ACA[2] reforms will depend upon increased access to clinical information for secondary purposes, in addition to coordination of care across settings and across time, increased exchange of information

[1] 76 Fed. Reg. 44512-4453 (July 26, 2011).
[2] Patient Protection and Affordable Care Act, P.L. 111-148 (2010).

with patients and caregivers, and computation of standardized measures of clinical quality – often for use in high-stakes payment and recognition programs.

We recognize, though, that this emerging electronic exchange environment may create new challenges for balancing reliable access to clinical data with protection of patient privacy and respect for individual patient preferences regarding data use, which suggests the need for substantial re-thinking of the historic approaches we have taken to encouraging and also regulating secondary uses of health care information.

We appreciate that the legal and ethical issues raised by human subjects research are very complex, and our comments will focus on several main issues raised by the ANPRM. We led the Tiger Team and Policy Committee, however, to focus on the following two questions only, as they were most relevant to work previously done by both:

1. What secondary uses of electronic health record data constitute "research" and therefore should be subject to regulation as research under the Common Rule (and under HIPAA)?
2. The ANPRM prioritizes consent (and also proposes the adoption of security measures) to safeguard EHR data (particularly identifiable EHR data) used for research purposes. Is this sufficient to build and maintain trust in secondary data uses?

Specifically, in considering these issues, the Policy Committee sought to build on its previous recommendations, which CDT also played a leading role in developing. These are taken verbatim from the letter approved by the Health IT Policy Committee in August 2010:[3]

*Core Values*

- The relationship between the patient and his/her health care provider is the foundation for trust in health information exchange; thus providers are responsible for maintaining the privacy and security of their patients' records.

- Patients should not be surprised about or harmed by collections, uses or disclosures of their information.

*Recommendations on Fair Information Practices and on Consent:*

- All entities involved in health information exchange should follow the full complement of fair information practices when handling personally identifiable health information.

- When the decision to disclose or exchange a patient's identifiable health information is not in control of the provider (or the provider's organized health

[3] *Available at*: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/hitpc_transmittal_p_s_tt_9_1_10.pdf.

care arrangement (OHCA[4])), patients should be able to exercise meaningful consent to their participation.

## II. High-Level Summary of Recommendations

With respect to the two questions considered by the Policy Committee (and identified above), we recommend that:

***Question 1*** (The discussion and recommendations regarding this question are relevant to ANPRM questions 24[5] and 45[6].)

- The use of a provider entities' EHR data for treatment purposes or to evaluate the safety, quality and effectiveness of prevention and treatment activities should not require consent or IRB approval or even minimal registration. HHS could take the approach of not labeling these activities as "research" but instead should consider them to be treatment or operations if conducted by, or on behalf of (such as by a business associate), a provider entity.
- The above exemption should apply only when the provider entity (or organized delivery system or OHCA) retains oversight and control over decisions regarding when their identifiable EHR data is used for quality, safety and effectiveness evaluations.

***Question 2*** (The discussion and recommendations regarding this question are relevant to ANPRM question 59[7].)

- The full complement of Fair Information Practices must be followed. Notice and consent are but two elements of FIPs and insufficient on their own to protect individuals' privacy.

---

[4] "Organized health care arrangement" (45 CFR 160.103) means: (1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider; (2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities: (i) Hold themselves out to the public as participating in a joint arrangement; and (ii) Participate in joint activities that include at least one of the following: (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk. [provisions applicable to health plans omitted]

[5] Question 24 contains numerous specific questions concerning the application of the Common Rule to activities such as quality improvement, public health and program evaluation studies. (76 Fed. Reg. at 44521.)

[6] Question 45 asks under what circumstances should future use of data initially collected for non-research purposes require informed consent. (76 Fed. Reg. at 44524.)

[7] Question 59 asks whether study subjects would be sufficiently protected from informational risks if investigators were required to adhere to a strict set of data security and information protection standards based on the HIPAA rules. (76 Fed. Reg. at 44526.)

***With respect to the additional issues contemplated by CDT, we recommend that:***

- Researches should be required to adopt mandatory security protections. All requirements must be commensurate and calibrated to privacy risks and, specifically, scaled to identifiability.
- There should be a distinction made between the risks associated with secondary use of identifiable data and use of de-identified data with respect to data specifically collected for research purposes.
- HHS should explore ways to make research uses of health data more transparent to patients and the public.
- In an effort to promote consistency, CDT supports the considered extension of the Common Rule to all research, whether or not Federally-funded, that is conducted at institutions in the United States that receive funding from a Common Rule agency for research with human subjects. We further support all efforts to harmonize the various rules and sets of guidance currently governing research activities.

These recommendations and the accompanying discussion below are relevant to ANPRM question 59,[8] the proposals regarding consent rules for excused research,[9] and ANPRM questions 71 and generally 72-74.[10]

Please note that the lack of comment on some aspects of the secondary use of data for research, such as the elements of informed consent and the circumstances justifying waiver of consent, should not be interpreted as CDT's support for, or disagreement with, the ideas in the ANPRM. We had insufficient time to consider those issues.

## III. Recommendations

### *Question 1: What secondary uses of EHR data constitute "research" and therefore should be subject to regulation as research under the Common Rule (and under HIPAA)?*

The Common Rule currently exempts research using existing EHR data from requirements for IRB review if the data does not identify individual subjects. The ANPRM proposes to retain this exemption from IRB review[11] – but to require prior, general consent for any research using identifiable data. Research done with a limited data set or with HIPAA de-identified data would not require consent.

---

[8] Id.

[9] 76 Fed. Reg. at 44519.

[10] Question 71 asks whether the applicability of the Common Rule be extended to all research that is *not* Federally funded that is being conducted at a domestic institution that receives some Federal funding for research with human subjects from a Common Rule agency; and questions 72 through 74 ask about existing differences in guidance on research protections from different agencies. (*See* 76 Fed. Reg. at 44528.)

[11] Instead, HHS is proposing to require researchers to file a brief one-page summary of the research with the IRB or research office. 76 Fed. Reg. at 44515.

Technology enhances the ability to conduct assessments of health care quality, safety and effectiveness; technology also enhances the ability of providers to effectively treat patients and improve population health. In its Health Information Technology Strategic Plan, ONC has specifically identified the goal of using health IT to improve both individual and population health.[12] Consequently, providers and health care organizations should be expected to use data in EHRs to optimally treat patients and evaluate the quality and effectiveness, including the comparative effectiveness, of the care they provide — *and to share the results of this analysis with others*. In practice, however, many health care organizations are today reluctant to engage in quality improvement efforts that require them to share information across enterprise boundaries, due to concerns deriving from uncertainty regarding what constitutes health care operations.

Current rules (both the Common Rule and HIPAA) define "research" as activities designed to develop or contribute to "generalizable knowledge."[13] Since the creation of a learning health care system will depend on more widespread dissemination of the results (in a way that safeguards individual privacy) of treatment interventions and evaluations of the health care system, characterizing research as any evaluative activity that contributes to the "generalizable knowledge" arguably no longer serves the interests of either patients or providers. We are concerned that the regulation of all such activities as "research" is so broad as to potentially limit or pose obstacles to them.

**We echo the Health IT Policy Committee in supporting HHS as it continues its efforts to modernize the Common Rule, create more consistency with HIPAA and address pertinent policy issues that arise with respect to secondary uses of EHR data. We would also like to reinforce the following suggestions made by the Policy Committee's recommendation letter:**

1. Exemption for Safety, Quality and Effectiveness Activities

The use of a provider entities' EHR data for treatment purposes or to evaluate the safety, quality and effectiveness of prevention and treatment activities should not require consent or IRB approval or even minimal registration. HHS could take the approach of not labeling these activities as "research" but instead should consider them to be treatment or operations if conducted by, or on behalf of (such as by a business associate), a provider entity.

This exemption should apply even if the results are intended to, or end up being, publicized or more widely shared (i.e., contribute to generalizable knowledge). Further, we expect provider entities to maintain proper oversight over, and be accountable for the conduct of, these activities, including when these activities are conducted by a business associate on their behalf. How provider entities govern the conduct of these activities within their practices or institutions should be left to their best judgment.[14]

---

[12] *Available* at: http://web.mediacdt.com/onc-emerg/FINAL-Federal-Health-IT-Strategic-Plan-0911.pdf.

[13] *See, e.g.,* 45 C.F.R. Sec. 164.501.

[14] It is quite possible that an entity might want to use its IRB to continue to have oversight into all evaluative activities done using information from its EHRs, and our recommendations should not

Consent should not be required to access EHR data for these safety, quality and effectiveness evaluation purposes, even if the data does not qualify as either a limited data set or de-identified data; however, provider entities should always use the minimum necessary amount of data to accomplish these activities (including removing patient identifiers prior to analysis for quality, safety or effectiveness when it is not necessary to identify individual patients).

Examples of the type of activities that we believe should be covered by this recommendation include (not intended to be an exhaustive list):

- The use of EHR data to improve care provided to patients (such as by evaluating the effectiveness of care).
- Early detection of patient safety issues through identification of patterns of adverse events.
- Evaluation of interventions designed to improve compliance with existing standards of care and outcomes (e.g. interventions that reduce the rate of hospital-acquired infections).
- Monitoring individual clinicians and professional staff for adherence to existing standards of care and existing treatment protocols; data comparisons of outcomes.
- Outreach efforts intended to increase patient compliance with existing standards (e.g. vaccinations, cancer screening tests).

2. Application of Research Exemption

Consistent with the HIT Policy Committee's previous recommendations (summarized earlier in this letter), the above exemption should apply only when the provider entity (or OHCA)[15]) retains oversight and control over decisions regarding when their identifiable EHR data is used for quality, safety and effectiveness evaluations.

This recommendation is based on previous Tiger Team/Policy Committee recommendations that recognize that patients place their trust in their health care providers with respect to stewardship of their health information. Consequently, when the provider entity (or the OHCA) that the patient trusts no longer has control over decisions regarding access to patient identifiable data (for example, in certain centralized health information organization (HIO) arrangements), the patient should have meaningful choices regarding whether or not his or her identifiable information is part of such an arrangement.

This exemption should be interpreted to allow provider entities (or OHCAs) to collaborate and share identifiable information for treatment purposes or to conduct quality, safety and effectiveness assessments, as long as the entities remain in control over decisions regarding how their EHR identifiable data is to be accessed, used and disclosed.

---

be interpreted to prohibit the use of IRBs for this purpose. However, we want to make it clear that we do not think the Common Rule should require such IRB review or registration.

[15] *Supra* note 4.

As described in greater detail below, entities should follow the full complement of fair information practices in using identifiable data for these purposes, including (but not limited to) being transparent with patients about how their data is used for treatment and quality, safety and effectiveness evaluation purposes; using only the minimum amount of data needed to accomplish the particular activity; and protecting the data with security measures that are commensurate with the risks to privacy).

In other words, rather than rely on the traditional IRB levels of review (or non-review) and general patient consent as a mechanism for regulating the use of EHR data for evaluative purposes, we urge HHS to hold provider entities accountable for developing and implementing their own policies in circumstances where these entities maintain oversight and control over the use of information from their EHRs. Such a viewpoint is consistent with the core value that patients generally trust their own providers with respect to privacy, and in particular for exercising good judgment regarding access to, and uses of, their sensitive health information. This view also acknowledges that requiring general patient consent for "research" does little to protect individual privacy (discussed in more detail below), and the ANPRM itself acknowledges that questions have been raised about the extent and quality of the protections afforded by current informed consent requirements and practices.[16]

It will be vital that federal guidance on privacy protective practices evolve with the continuing changes in health policy and technology. As HHS refines its policies on research, we encourage you to anticipate these and similar "secondary uses" of patient health information and provide as much and as specific guidance as possible to practitioners, both to reduce unnecessary concern, and to facilitate beneficial uses of these data while protecting individual privacy. There are doubtless certain types of quality-, safety- and effectiveness-related activities that should still be regulated as research, such as, for example, "prospective" reviews of EHR data, versus a retrospective look back at care that was given outside of the context of a research protocol. Given the sensitivity of this issue and the potential for controversy, we urge HHS to spend additional time considering this question of what constitutes "research" and what is "operations" prior to issuing a proposed or final set of research rules, thinking about how to set some sort of litmus test for regulation – such as the degree of comfort associated with having a particular activity written about on the front page of the local newspaper.

***Question 2: The ANPRM prioritizes consent (and also proposes the adoption of security measures) to safeguard EHR data (particularly identifiable EHR data) used for research purposes. Is this sufficient to build and maintain trust in secondary data uses?***

The Common Rule has traditionally focused on when an individual's consent is or is not required to be obtained for research uses of clinical data, and the ANPRM largely continues this historic emphasis (with the exception of the suggested addition of security requirements, which we support and address further below). However, consent is but one element of fair information practices, the framework that typically is applied to uses of potentially sensitive information.

[16] 76 Fed. Reg. at 44513.

Notice and consent do arguably serve to make patients more aware of the potential for use and disclosure of their information, but they do very little on their own to protect individuals' privacy. In isolation, without other legal limits, mandating consent is more likely to lead to over-broad information sharing than to the protection of patient privacy. Further, overreliance on consent can have the effect of inappropriately shifting the burden for protecting privacy onto patients, particularly when consent is sought in a general or "blanket" way (such as consent for all "research" uses of EHR data).[17]

Though the focus of the ANPRM in its consent discussion is mainly on the quality and understandability of the consent forms, instead there should be a more explicit acknowledgement of the insufficient privacy protections afforded by a pure reliance on consent. Rather than introduce the potential for bias by requiring a general consent that will be of little value in really protecting an individual's privacy, [18] HHS should focus on robust accountability for the entities that conduct these types of analyses and ideally greater transparency to the public that such quality, safety and effectiveness evaluations using EHR data are done routinely and in privacy-protective ways.

**We offer the following suggestions regarding the necessity of HHS imposing additional protections on data beyond consent:**

Although security safeguards and meaningful consent certainly are important, we urge HHS to think more broadly when it comes to data protection. Specifically, as mentioned above, the *full complement* of Fair Information Practices must be required to be followed. We have consistently endorsed ONC's articulation of FIPs, the principles of Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.[19] These include:

- ***Individual Access*** – Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
- ***Correction*** – Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.
- ***Openness and Transparency*** – There should be openness and transparency about policies, procedures and technologies that directly affect individuals and/or their individually identifiable health information.
- ***Individual Choice*** – Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and

[17] For a more extensive discussion of the dangers of overreliance on consent, see CDT's January 2009 paper, "Rethinking the Role of Consent in Protecting Health Information Privacy," *available at*: http://www.cdt.org/files/pdfs/20090126Consent.pdf.

[18] This point is relevant to ANPRM question 49, which asks whether it is desirable to implement the use of a standardized, general consent form to permit future research on data.

[19] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf.

disclosure of their individually identifiable health information. (This is commonly referred to as the individual's right to consent to identifiable health information exchange.)

- ***Collection, Use and Disclosure Limitation*** – Individually identifiable health information should be collected, used and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
- ***Data Quality and Integrity*** – Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
- ***Safeguards*** – Individually identifiable health information should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability, and to prevent unauthorized or inappropriate access, use or disclosure.
- ***Accountability*** – These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

We strongly recommend that all entities using clinical data for secondary and research purposes be required to adopt policies and/or best practices that address *all* of the relevant fair information practices above, *regardless of whether or not a patient's consent is required to be obtained*.

FIPs are intended to be flexible and contextual, and not rigid rules applied without consideration for the particular circumstances and potential consequences. We recognize that not all of the fair information practices may be relevant to some researchers (for example, the requirement to provide individuals with access to copies of information about them or to provide a mechanism for correcting data). But we do believe it is relevant for researchers to limit the amount of information collected to what is necessary to perform the research; limit the number of people who have access to the data for research purposes to those performing the research; have policies for being open and transparent with the public about research that is conducted using clinical data; and adopt and adhere to specific retention policies with respect to the data.

### *CDT-Specific Recommendations*

1. Security Protections

We applaud the ANPRM for its recommendation that researchers be required to adopt security protections and urge that this provision be included in subsequent rulemakings on this topic. Protection of individually identifiable health information with safeguards to ensure its confidentiality and integrity, and to prevent unauthorized or inappropriate access, use or disclosure, is one of the fair information practices discussed above, and we strongly support this consistency.

In particular, we support HHS' proposed adoption of HIPAA Security Rule provisions, including the requirement of mandatory security and information protection standards and rules protecting against the re-identification of de-identified information.

With respect to security, however, we feel strongly that all requirements be calibrated to the privacy risks of the particular data set. In particular, security requirements should be scaled to identifiability, with the acknowledgment that all data, with respect to identifiability, are not equal in terms of privacy risk. The need for identifiable data to have greater protections than de-identified data is discussed at greater length below.

2. Necessary Distinction Between Secondary Use of Identifiable Data and De-Identified Data With Respect to Data Specifically Collected for Research Purposes

With respect to data originally collected for *research* purposes, we are concerned about the ANRPM's proposal that *consent would be required regardless of whether the researcher obtains identifiers*.[20] This would be a major change with regard to the current interpretation of the Common Rule in cases where the researcher did not obtain identifiers, and would mean that where research information with identifiers is then de-identified, it would no longer be allowably used for secondary purposes to which the subjects did not consent.

CDT has long believed that it is important that HIPAA and other health privacy laws maintain a distinction between fully identifiable data and data that has been properly de-identified – i.e., sufficiently striped of identifiers that there is no reasonable basis to believe the information can be re-identified. If privacy laws do not recognize a distinction between de-identified and fully identified data, then there will be little or no incentive to de-identify data and learn to work with it, or to improve de-identification techniques – which are powerful tools for protecting patient privacy. Instead, there will be a tendency to use fully identified data for secondary purposes such as public health and quality control, which would raise far greater privacy risks for individuals. We are wary of undermining the current framework in which it is allowable to conduct research using de-identified data, or a limited data set, without having obtained patient consent.

[20] 76 Fed. Reg. at 44519.

Further, we are concerned by the ANPRM's tacit acceptance of the idea that there is a "fluid" line between what constitutes de-identified and identifiable data.[21] This creates the danger mentioned above: that treating the two categories of data as the same, or at least not substantially different for purposes of secondary use, removes the incentive to de-identify data, and ignores the reality that data that has been stripped of identifiers poses fewer and less dangerous privacy risks as does data that contains personal identifiers.[22] That is not to say that there is *no* risk of re-identification, however, and requiring data recipients to commit not to re-identify data, as proposed in the ANPRM, provides another good set of protections.

In general we support reliance on HIPAA standards for de-identification,[23] but we also urge HHS to consistently review this standard to ensure it continues to result in a very low risk of re-identification.[24] As discussed again below, we urge HHS to strive where possible for consistency, but this focus must be accompanied by an insistence that both HIPAA and the Common Rule follow appropriate and strong standards. We further agree with the ANPRM that, in light of emerging technologies and evolving information risks, it is advisable to regularly evaluate the standards and methodologies for de-identification under both the Common Rule and HIPAA.[25]

3. Greater Promotion of Transparency

CDT urges HHS to give more consideration in future rules or guidance on research on how to promote greater transparency to patients and the public about research activities. Individuals are more apt to mistrust what they do not know or do not understand, and building public trust in research will require more careful attention to not surprising patients regarding uses of their health data. As noted above, consent can sometimes serve the role of educating patients about research uses, but since it does little to genuinely protect privacy, and may pose obstacles to more robust analysis of EHR data, HHS should actively explore other options for promoting transparency.

4. Promotion of Consistency

CDT supports the ANPRM's consideration of the extension of the Common Rule to all research, whether or not Federally-funded, conducted at institutions in the United States that receive from funding from a Common Rule agency for research with human subjects.[26] Extending protections to greater numbers of individuals than are reached now is a positive development that we encourage HHS to pursue. There is great benefit to be derived from consistent rules and the required application of the above-discussed fair information principles to a greater number of entities conducting research.

---

[21] 76 Fed. Reg. at 44524.
[22] For a discussion of the role of de-identification in protecting individual privacy, see http://www.cdt.org/paper/memo-sorrell-v-ims-health-inc-supreme-court-case-requires-nuanced-understanding-privacy.
[23] 76 Fed. Reg. at 44525-44526.
[24] For more information, see CDT's paper on HIPAA de-identification, http://www.cdt.org/paper/encouraging-use-and-rethinking-protections-de-identified-and-anonymized-health-data
[25] *See, e.g.,* 45 C.F.R. Sec. 164.514(b).
[26] 76 Fed. Reg. at 44528.

Further, we support the ANPRM's stated goal of clarifying and harmonizing regulatory requirements and agency guidance. Clarity and consistency will promote research; in contrast, confusion regarding applicable or relevant law can have the chilling effect of stifling innovation and hampering scientific progress. We urge HHS to fulfill the intent of the proposed revisions by being as unambiguous and uniform as possible with respect to data use rules, regulations and guidance.

## IV. Conclusion

We appreciate the opportunity to provide these recommendations and look forward to discussing next steps.

Sincerely yours,

Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology