



January 14, 2013

Submitted electronically

Office of the National Coordinator for Health Information Technology
HIT Policy Committee
Department of Health and Human Services
Patriots Plaza II, 355 E Street, SW
Washington, D.C. 20201
RE: Request for Comment – Stage 3 Definition of Meaningful Use

Dear HIT Policy Committee:

The Center for Democracy & Technology (“CDT”) is a non-profit Internet and technology advocacy organization that promotes public policies that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, CDT, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education, and litigation, as well as through the development of industry best practices and technology standards. Recognizing that a networked health care system can lead to improved health care quality, reduced costs, and empowered consumers, CDT is using its experience to shape workable privacy solutions for a health care system characterized by electronic health information exchange.

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 the U.S. Congress five times since 2008 on the privacy and security issues raised by health IT, and we chair the privacy and security policy working group of the federal Health IT Policy Committee (called the “Tiger Team”).

CDT is a member of the Consumer Partnership for eHealth (CPeH) and has signed onto its comment letter. This letter reflects a number of additional thoughts and suggestions that we independently want to convey. In particular, we provide recommendations regarding the following subjects:

- View/Download/Transmit functionality;
- Patient-generated health information;
- Ability to request an amendment through an online portal;
- EHR query capability;
- Privacy and security, including identification, authentication and accounting of disclosures;

- Patient identity matching; and
- Consent management.

I. View/Download/Transmit – SGRP 204A

CDT has consistently and heartily endorsed the Meaningful Use and Certification provisions that will provide patients with the ability to view, download and transmit electronically their health information (referred to herein as “V/D/T”), as well as to engage in secure e-mail exchange with their clinical care providers. This was a monumental advancement for consumers in Stage 2 of the incentive program, and we applaud and support each of the proposed Stage 3 advancements of this criterion.

In particular, as ONC suggests, we see great potential value in giving credit to providers (e.g. specialists) for V/D/T if they send – or enable their patients to download and transmit – information to a location of the patient’s choosing (e.g.: primary care provider or non-provider affiliated personal health record). This signals a real-world understanding of how this technological capability would work in practice, as well as of the benefits of patient-directed information flows.

With respect to the Stage 3 V/D/T criteria and its related components, we offer the following recommendations.

A. Transparency

One of the numerous benefits of widespread V/D/T functionality will be increased transparency of health information and health information exchange to patients and their care team. We note that the Health IT Policy Committee’s (HITPC) Privacy & Security Tiger Team recently developed recommendations regarding transparency and the view/download/transmit functionality, specifically urging that providers offer guidance to patients with respect to the benefits and risks of the use of such capabilities. CDT played a lead role in developing these recommendations, which were in large part based upon guidance issued by the Markle Foundation,¹ and we rearticulate them here:

- With respect to the **download functionality**, guidance to patients should be offered at the time the patient indicates a desire to download electronic health information and should, at a minimum, address the following three items: (1) remind patients that they will be in control of the copy of their medical information that they have downloaded and should take steps to protect this information in the same way that they protect other types of sensitive information; (2) include a link or links to resources with more information on such topics as the download process and how the patient can best protect information after download; and (3) obtain independent confirmation that the patient wants to complete the download transaction or transactions.

¹ The Markle Foundation, (2010). Policies in Practice 1: The Download Capability, *available at*: http://www.markle.org/sites/default/files/20100831_dlcapability.pdf.

- With respect to the **view functionality**, patient guidance should address the potential risks of viewing information on a public computer, or viewing sensitive information on a screen that may be visible to others, or failing to properly log out after viewing. Providers should also: (1) utilize techniques, if appropriate, that avoid or minimize the need for patients to receive repeat notices of the guidance on view and/or download risks; (2) request vendors and software developers to configure the view and download functionality in a way that no cache copies are retained after the view session is terminated; and (3) request that their view and download functionality include the capability to automatically terminate the session after a period of inactivity.

The full set of relevant Tiger Team recommendations is available at <http://www.healthit.gov/policy-researchers-implementers/health-it-policy-committee-recommendations-national-coordinator-heal> (August 2011).

B. Automated Transmit

With respect to the “automated transmit” proposed menu item, we strongly support the ability of patients to designate to whom and when a summary of care document is sent to a patient-designated recipient. We further support the HITPC’s pledge to review the results of the Automated Blue Button Initiative (“ABBI”) pilots as they relate to this proposal.

CDT has participated in both the Push and Pull Working Groups in the ABBI and our primary areas of focus have been ensuring that:

- Patients have access to all elements of the summary of care document through the vehicle of a machine-readable consolidated-CCD document and that this data is transmitted with a “transform” that commonly-available software (e.g., web browsers) can use to translate the record into a human-readable presentation format;
- The patient-designated “recipient” of this document may not be a person but could also be an *application* such as a personal health record (PHR) or a mobile health application; and
- The requirements for applications and Health Information Service Providers (HISPs) to receive a summary of care document as transmitted be simple but robust. That is, there should be no barriers that prevent small developers working in the proverbial “garage” from creating innovative services and applications that securely compute, store and even transfer health data to other caregivers. At the same time, these requirements should adequately promote scalability, interoperability and the integrity of patient health information.

We urge the HITPC to keep these principles in mind when it reviews the ABBI pilots. For example, the policies and procedures governing the “trust bundle” that will store encryption keys for encrypting V/D/T emails to patient-designated recipients is a work in progress but will be crucial to creating an innovative patient health information ecosystem.

II. Provide 10% of Patients with the Ability to Submit Patient-Generated Health Information – SGRP 204B

CDT fully supports the new Stage 3 criterion that offers patients the ability to contribute information directly to their medical record. Improved performance on high-priority medical conditions and patient engagement in their health and health care are important goals, and this measure will be an effective step toward achieving both.

A significant focus of this next stage of Meaningful Use should be identity-proofing and authentication methods for patient access to web portals. The quality of information is only as good as its accuracy, and adding patient-generated information to the electronic health record serves to heighten such concerns. Thus ONC should adopt and disseminate best practices to eligible providers, eligible hospitals, critical access hospitals and vendors regarding identity-proofing and authentication.

As recommended by the Privacy and Security Tiger Team, identity-proofing and authentication best practices should:

- Be commensurate with risks;
- Be simple and usable for patients and consistent with “what they are willing to do”;
- Be flexible — “one size does not fit all”;
- Leverage solutions in other sectors, such as banking;
- Be accompanied by education that make these processes transparent to the patient;
- Be built to scalable solutions (e.g., greater use of voluntary secure identity providers); and
- Be able to evolve over time as technology changes.

The full list of Tiger Team recommendations regarding identity-proofing, authentication, transparency and DIRECT-enabled transmit can be read here:
<http://www.healthit.gov/policy-researchers-implementers/hit-policy-committee-12>.

III. Provide Patients with the Ability to Request an Amendment to Their Record Online Through a Patient Portal in an Obvious Manner – SGRP 204D

CDT is pleased with the new Stage 3 criterion that would provide patients with an ability to request an amendment to their health record online. The criterion helps to ensure the accuracy and reliability of data stored in an EHR, while simultaneously enabling the engagement of patients and their caregivers in their own health and care. Further, this capability will help support providers’ compliance with the HIPAA Privacy Rule.

Once the V/D/T functionality is more fully implemented, patients will on occasion identify errors in or seek revisions to their records. This is an important check on accuracy, but also means providers will need to be prepared with a process for handling error identification and correction. We urge ONC and CMS to explore whether there is a certification capability that would allow a patient-facing portal to request – and then transmit – an amendment to a health record. As we have noted in previous comment

letters, providers too will need the capability to transmit amendments (or appended or rebuttal information) to others who have the incorrect or disputed data.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule already requires covered entities to make reasonable efforts to provide an amendment to persons identified by the patient as needing to receive the amendment, as well as persons or entities that the covered entity knows previously received the information to be corrected and might “foreseeably rely on the information to the detriment of the [patient].”² This new capability would enable certified EHR technology to support providers in complying with this portion of the Privacy Rule, while at the same time engaging patients in the process.

Finally, as the HITPC, and ultimately ONC and CMS, determine how to implement this objective, it will be critical to ensure that in any cases where the patient’s requested amendment is not accepted into the medical record, patients are offered an explanation as to why. If patients are able to directly make the request for amendments, they should also be entitled to direct feedback through the same communication channel.

IV. The EHR must be able to query another entity for outside records and respond to such queries – IEWG 101

Ensuring high-quality care for a patient will depend on good reliable data, coming either from the treating provider’s medical records or elsewhere. Establishing the capability of providers to query patient data from other sources can help assure that providers have the information they need to appropriately care for the patient.

However, the capability to query information about a patient triggers important policy questions that have significant privacy implications. The Privacy and Security regulations promulgated under HIPAA set rules for how health care providers can use and disclose identifiable health information about their patients; but the regulations do not set rules for how information about a patient can be *collected* from other sources. Consequently, it is critical for HHS to develop policies on query prior to implementing widespread EHR query capability.

The Tiger Team is beginning to address this issue and will hopefully issue recommendations on querying of patient records within the first quarter of 2013. Any query certification criteria for certified electronic health record technology will then need to be reconciled with policy.

V. Privacy and Security

A. How can the HITPC’s recommendation be reconciled with the National Strategy for Trusted Identities in Cyberspace (NSTIC) approach to identification, which strongly encourages the re-use of third-party credentials? – PSTT 01

² 45 C.F.R. § 164.526(c).

The HITPC expressly endorsed the NSTIC approach for credentialing of both providers and patients for EHR access, and CDT also is hopeful that efforts to create an identity ecosystem that will reliably issue secure and interoperable credentials through trusted third-party identity providers will be successful. Reliance on such third-party credentials could reduce burdens on providers and provide greater security for health information exchange.

However, it is currently unclear when and if the work of NSTIC and its Identity Ecosystem Steering Group (IDESG) will result in standards and other products specifically useful to HIT; it could be years before this ecosystem exists and reliable credentials are widely available to both providers and patients. To assure the capability to exchange health information among providers and patients by the beginning of Stage 2 of Meaningful Use and continuing into Stage 3, it will be critical for providers to have the capability to issue reliable, MU2-compliant credentials to both clinicians and patients. The HITPC recommendations should help facilitate this short-term fix, while enabling and monitoring the development of more effective long-term solutions.

B. How would ONC test the HITPC’s recommendation re: two-factor (or higher) authentication for provider users to remotely access PHI in certification criteria? – PSTT 02

Two-factor authentication requires the use of “something you have” in addition to something you know (customarily a username and password) in order to authenticate an individual. The HITPC has acknowledged that there are a variety of ways to implement a second authenticating factor, which provides vendors with a range of potential options to meet the needs of their customers. Given this flexibility, certification should focus on testing the approach that the vendor has implemented and making sure that it functions as intended and minimizes risk.

In terms of minimizing risk, certification requirements should specify that vendors describe the functionality of their solutions fully,³ and any required security analysis of the larger EHR product needs to explicitly include the detailed authentication mechanism in terms of threats, protections and evidence that the authentication mechanism was in scope for any adversarial vulnerability testing (“penetration testing”). ONC could also consider providing vendors with certification “credit” if they have implemented a second or third factor that is listed in the most recent version of NIST 800-63.⁴

³ Authentication is a technical area of system security where it does not promote security to have proprietary or secret mechanisms, models and/or algorithms. Here, these elements should reference existing standards or describe the solution in enough detail such that an expert can make an independent determination of the adequacy of the solution.

⁴ At the time of writing the most recent version of this document was version 1, superseding the original version. See: “Electronic Authentication Guidance”, National Institute of Standards & Technology, Special Publication 800-63-1, 2011, *available at*: <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

C. Should ONC permit certification of an EHR as stand-alone and/or an EHR along with a third-party authentication service provider? – PSTT 03

If a vendor chooses to use (or offer) a third-party authentication service provider, the authentication technology used by that third-party should ideally be tested in the same way that technology would be tested if it were offered directly by the EHR. Ultimately, if the efforts to implement NSTIC result in trusted third-party credentialing processes, potentially those could be relied on in lieu of requiring certification. The goal should be to avoid incorrect implementation of standardized third-party authentication provision by certification testing of the EHR as it will be used.

D. What, if any, security risk issues (or HIPAA Security Rule provisions) should be subject to Meaningful Use attestation in Stage 3? – PSTT 04

The HHS Office for Civil Rights (OCR) has significantly stepped up its enforcement of the HIPAA regulations, from collecting monetary settlements for alleged HIPAA violations from an increasing number of providers to performing compliance audits of both covered entities and business associates. These settlements and the audits will yield important information on the most common HIPAA Security Rule provisions that are not being adequately addressed by HIPAA-covered providers or their business associates. OCR should help advise the HITPC, ONC and CMS on these commonly neglected Security Rule provisions, and those should be included in Stage 3 Meaningful Use attestation.

E. Accounting of Disclosures – PSTT 05-08

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).⁵ Openness and transparency about personal information access, use and disclosure is a fundamental tenet of FIPs, and integrating an accounting for disclosures requirement into Meaningful Use via EHR certification provides a vehicle for such transparency. A recent survey by the Markle Foundation indicates that both doctors and the public strongly support letting patients see who has had access to their records,⁶ and requirements to account for disclosures provide a vehicle for greater transparency into how an individual's information is actually accessed, used and disclosed.

⁵ 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. 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 Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.

⁶ 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, *available at*: <http://www.markle.org/publications/1461-public-and-doctors-overwhelmingly-agree-health-it-priorities-improve-patient-care>.

With respect to ONC's technological questions, ASTM E-2147-01, "Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems," seems to be particularly well-suited for a certification-based requirement for EHR systems. It specifies both the content and format of system access logs to protected health information (PHI) in health information systems such as EHRs. It also addresses the maintenance requirements of keeping a single log of PHI access in an EHR across multiple systems for provision to external parties, including the patient.

As for a specific time period requirement for EHR certification criteria for the maintenance of such log files, we note that the time period for maintaining an accounting of disclosures is currently six years⁷ — until a new Accounting of Disclosures rule is promulgated by OCR, we would encourage a lengthy attestation period.⁸

With a highly dependent, system-level technical element in EHRs such as audit logs, it is essential that the policy governing their content, use and maintenance be developed in concert with the technical standards. CDT has remarked in the past that policy created with an indirect connection to the underlying standards and technology risks creating artifacts that the market cannot support in an efficient and economical manner⁹ and that might miss advancements in both policy and technology that a more harmonized process would include by nature.

VI. ONC Addendum

A. What could facilitate identity matching – query, e.g. maintain external patient id, standards for matching attributes – ONC02

The HITPC's recommendations for improving the accuracy of patient matching included some specific technical requirements with respect to demographic data fields; ONC should ensure that those recommendations are being implemented through certification.

In addition, the Bipartisan Policy Center also recently released recommendations on actions to accelerate health information exchange, and those recommendations include a focus on improving patient matching accuracy.¹⁰ Of note, those recommendations suggest that the efforts to implement NSTIC and provide individuals with a trusted identity for use in on-line transactions could yield some potential solutions for improving matching accuracy. ONC should explore those recommendations further, and

⁷ 45 CFR § 164.528)

⁸ Section 13405(c)(1)(B) of HITECH specifies a three-year period for disclosures related to treatment, payment and health care operations. OCR sought to harmonize the existing six year regulatory requirement with this stipulation in 2011's Accounting of Disclosures rulemaking (76 Fed. Reg. 31426 at 31430).

⁹ See Center for Democracy and Technology, "Comments on OCR NPRM on the HIPAA Privacy Rule and Proposed Accounting of Disclosures under HITECH", August, 2012, at 3, *available at*: https://www.cdt.org/files/pdfs/CDT_Comments_to_HHS_Accounting_of_Disclosures_NPRM.pdf.

¹⁰ See *Accelerating Electronic Information Sharing to Improve Quality and Reduce Costs in Health Care*, *available at*: <http://bipartisanpolicy.org/news/press-releases/2012/10/bipartisan-policy-center-calls-collaborative-action-accelerate-electroni>.

encourage a greater focus by providers as well as by agencies within HHS on resolving this issue.

B. For the objective identified as SGRP 204B, what information would providers consider most valuable to receive electronically from patients? What information do patients think is most valuable as an initial minimum set for patients to send to providers electronically outside the clinical visit? What other data could be added in the future? – ONC04

On this topic we agree with the comments submitted by CPeH and the National Program Office of Project HealthDesign.

C. Consent management – ONC08

With respect to ONC's questions about consent management, CDT recognizes that these are challenging but important ones to ask. Meaningful Use is not the most effective or appropriate vehicle for advancing or creating new consent policy. However, it does have the potential to improve the capacity of EHR infrastructure to manage consent by imposing certification criteria that enable providers, regardless of their state, to meet their legal obligations when it comes to obtaining and recording patient consent.

More broadly, patients' ability to control the use and disclosure of certain elements of their health record is a matter of *policy* and should be determined through a robust policymaking process. Policy on consent should not be set merely through the adoption of a particular technical standard. To the extent the Meaningful Use certification standards adopt metadata privacy standards, such standards should focus on supporting policies already in existence that provide patients with granular consent rights, such as the laws governing the disclosure of certain identifiable substance abuse treatment records, the state laws that require consent for the sharing of certain categories of sensitive health data, and the right established in HITECH that allows patients to restrict the sharing of their data with health plans when they pay out-of-pocket for their care.

It is also critical to manage patient expectations when it comes to consent. A metadata tag indicating a patient preference does not necessarily translate into a legal obligation for that preference to be honored. Further, it is typically the laws that govern the receiving institution that control how data is treated once it has been transmitted, and thus patients should not expect their consent wishes to be honored downstream.¹¹

The presence of a metadata tag with a consent preference allows a data discloser (such as a health care provider) to indicate that the required consent to share the data has been obtained; the tag also puts a recipient of a patient's data on notice that the patient has expressed a preference with respect to the sharing of that data. However, if the

¹¹ It should be noted that the federal substance abuse laws are an exception to this general principle because they cover re-disclosure of information by downstream recipients. We note as well that some state laws may also bind downstream recipients, although these laws will likely only be binding by those within that state's jurisdiction.

recipient is not bound by a legal obligation to obtain consent before further using or sharing that data, the presence of the metadata tag will not create a legal obligation to honor the preference. For example, if a patient sends health information to her physician, and the information includes a metadata tag that indicates that the data cannot be disclosed to others, that physician is only legally bound to honor the metadata tag if they are subject to a binding legal requirement to obtain the patient's consent prior to further access, use and disclosure of the data.

None of this is should be construed to negate the importance of creating standards that will enable granular consent policy to be honored. If electronic health records are unable to honor current policies, they will be far less useful to providers who are already required to comply with them. Certification of EHRs is an ideal vehicle for encouraging the adoption of such functionality.

VII. Conclusion

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

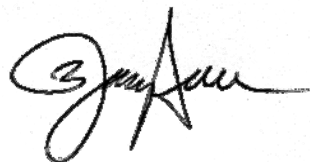
Respectfully submitted,



Deven McGraw
Director, Health Privacy Project CDT



Alice Leiter
Policy Counsel, Health Privacy Project CDT



Joseph Lorenzo-Hall
Senior Staff Technologist, CDT