Health IT Policy Committee
A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

June 10, 2014
Karen DeSalvo, MD
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. DeSalvo:

The HIT Policy Committee (Committee) gave the following broad charge to the Privacy & Security Tiger Team (Tiger Team):

Broad Charge for the Privacy & Security Tiger Team
The Tiger Team is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee (HITPC) on privacy and security policies and practices that will help build public trust in health information technology and electronic health information exchange (HIE), and enable their appropriate use to improve healthcare quality and efficiency, particularly as related to American Recovery and Reinvestment Act (ARRA) and the Affordable Care Act (ACA) which mandates a number of duties to the Office of the National Coordinator (ONC) relative to privacy and security.

The Privacy and Security Tiger Team considered friends and family and personal representatives' access to patients' electronic health information through view, download and transmit (VDT) functionality in certified EHR Technology (CEHRT). In support of this effort, the Tiger Team invited public comment through the ONC Health IT Buzz Blog and the insights provided helped to inform the deliberations. (A summary of these comments is included as attachment I.) This letter provides the resulting recommendations, which were adopted by the Committee on April 8, 2014, to the National Coordinator, Department of Health and Human Services (HHS).

Background
Under the HIPAA Privacy Rule, a person authorized (under State or other applicable law, e.g., tribal or military law) to act on behalf of the individual in making health care related decisions is the individual's "personal representative." Subject to certain exceptions, the Privacy Rule requires covered entities (CEs) to treat an individual's personal representative as the individual with respect to uses and disclosures of the individual's protected health information (PHI), as well as the individual's rights under the Rule. The Privacy Rule also currently permits (but does not require) CEs to share PHI with family members or other persons who are involved in the individual's health care or payment for care (friends and family). In this case, PHI that may be disclosed is information directly relevant to the friend or family member's

involvement with the individual's care or care payment and individuals have the right to object to (and prevent) such disclosures.[1]

One of these ways in which this information may be shared is through VDT, a capability required by meaningful use. Because legal personal representatives stand in the shoes of the patient with respect to accessing PHI, they may have an interest in exercising their legal right to access the patient's PHI by using VDT. Additionally, in line with their right to expressly authorize the sharing of their PHI with others, patients will have an interest in friends and family having access to their PHI through VDT.

That said, before a CE grants VDT access to someone other than the patient, they must first determine whether the person is legally authorized to access the patient's PHI through VDT, either due to authorization from the patient (friends and family) or due to legal status (personal representative). Identification and authentication of the individual or entity being granted access (are they who they say they are) and education of patients and providers on the rights, responsibilities, and limitations of VDT are also key.

It is also worth noting that absent a mechanism for granting friends and family and personal representatives access to VDT, patients may facilitate such VDT access on their own by sharing their user names and passwords. As a result, the process for granting credentials to authorized friends, family and personal representatives should be sufficiently easy to discourage shared access yet still be sufficient to satisfy the need to assure authorization and identification/authentication. Education of patients about why sharing passwords is not advisable (e.g. less capability to determine who has taken action in VDT) is also important, although it is acknowledged that what patients will do with such information is beyond the control of the CE.

Best Practice Recommendations

The Tiger Team urges ONC to develop and disseminate the following best practices for assuring that access to adult patient[2] VDT be extended to friends and family authorized by the patient, and, where appropriate, legal personal representatives. The Tiger Team's recommendations build on those that it has previously expressed[3] and focus on:

- Authorization of (1) personal representatives and (2) friends and family,

[1] Note that in emergencies and other circumstances, covered entities may make reasonable inferences and act in the best interests of the individual with respect to PHI disclosures to friends and family.

[2] Please note that the proxy access to minors' accounts is not within the scope of the current letter or the proposed best practice recommendations. The Tiger Team plans to separately deal with minors' privacy issues in future discussions.

[3] Prior relevant recommendations include those on "View and Download Best Practices" (8/16/11 HITPC Transmittal Letter, http://www.healthit.gov/FACAS/sites/faca/files/HITPC_PSTT_Transmit_8162011.pdf), "Identity Proofing and Authentication" (5/3/13 HITPC Transmittal Letter, http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_050313_pstt_recommendations.pdf), and "Query/Response" (8/21/13 HITPC Transmittal Letter, http://www.healthit.gov/facas/sites/faca/files/HITPC_Transmittal_08212013.pdf).

- Identity proofing and authentication,
- The scope of VDT access, and
- Education.

Whether someone qualifies as a "personal representative" depends on state law and permutations in these laws make it difficult to make uniform national policy/best practices. Nonetheless, providers should consider whether and how they can adapt the processes they currently use for granting VDT access to patients to grant personal representative access to records. It would also be helpful for providers to have the capability to store documentation of personal representative status.

For friends and family, the Tiger Team focuses its recommendations on two use cases.[4] The easier case in this context is when a patient makes a request for VDT access for a friend or family member. In such a case, the Tiger Team recommends the following best practices:

- The provider should have the ability to fulfill the request either in person or remotely (for example, over the phone, through VDT if that functionality is provided, via e-mail, etc.)
- Providers should document the request (the capability to store this documentation electronically would be helpful).
- Out-of-band notification can be used to notify/confirm changes in VDT access with patients. This is particularly important when a patient's request for proxy access is made remotely or through software acting on the patient's behalf.

The harder case is when a friend or family members makes the request for VDT access. In this case, such access must be confirmed with the patient, such as through out-of-band confirmation. If the patient is incapacitated, the provider will need to consider whether providing access to VDT is appropriate; it should be remembered that HIPAA permits the sharing of information with friends or family in such a case, but the information that can be shared is limited to that which is relevant to treatment.

For identity proofing and authentication, patients can provide credentials or directly authorize VDT access (for example, through VDT or by separate communication of contact information). Previous best practices regarding identity proofing and authentication[5] also apply here. In addition, the provider also needs to develop a process and capability to cut off VDT access by friends, family and personal representatives due to a patient change in preferences or a change in personal representative legal status.

In terms of scope of VDT access, the Tiger Team notes that VDT accounts may offer more than "all or nothing" access for proxies with both respect to data content and functions that can be performed. In line with this, it is important to educate patients on whatever options are available for friends/family access so they can make informed decisions about the scope of proxy access to be granted. For example, providers may want to alert patients that certain types of options would enable family members (who

[4] It is acknowledged that a number of other cases exist.
[5] http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_050313_pstt_recommendations.pdf

are provided VDT accounts) to see information that a patient has reported as family medical history. Education on the scope of data that will be accessible by anyone granted proxy access is also particularly important in "all or nothing" contexts. For personal representatives, providers need to determine whether VDT access can be limited to what the personal representative is authorized to access prior to establishing a VDT account for the personal representative. Advance directives and other documents may play a role in establishing personal representative status and the scope of a personal representative's authority. If a provider cannot limit a personal representative's access in VDT to the information the personal representative is authorized to access under law, VDT access may not be grantable.

The Tiger Team also suggests the following in regard to general education:

- The ONC should disseminate best practices to providers, to help them to establish (and turn off) proxy access to VDT accounts consistent with the law and patient needs. This includes planning for scenarios such as a patient's change in preference, change in personal representative status, or the patient's death—In which event, some proxy access should be restricted or disabled, for example, the proxy's ability to fill prescriptions.
- ONC's VDT proxy access educational materials should be developed in a way that is broadly applicable to providers and other office staff who may play a role in informing patients about the benefits/risks of proxy access or in managing patient proxy access.
- Providers should educate their patients on the risks and benefits of VDT, consistent with the HITPC's prior recommendations,[6] and such education should include the risks/benefits of proxy access, what information is accessible to friends and family (e.g., family history), and what functions are available to friends and family in the portal, including (if applicable) download and transmit. Given the enormity of the task of educating patients, ONC may also want to consider using available communications channels—such as publicly available videos—to educate patients on the benefits and risks of permitting proxy access.

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

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee

[6] http://www.healthit.gov/FACAS/sites/faca/files/HITPC_PSTT_Transmit_8162011.pdf

Attachment I: Summary of Health IT Buzz Blog Comments Regarding Friends and Family/Personal Representative Access Via View, Download, and Transmit

The Tiger Team's February 3, 2014 post on the Health IT Buzz Blog solicited public comments on current practices and stakeholder concerns on authorization, authentication, and granularity of access with respect to friends, family, and personal representative access to VDT accounts. More than 40 comments were received. The following summarizes the key comments.

Views on Authorization

- Commenters reinforced the practice of written (signed) authorization from the patient and personal representative as the only means to maintain HIPAA compliance to release information. This was reviewed in conjunction with acceptable forms of identification.
- Commenters compared and contrasted authentication in banking to electronic healthcare records (e.g. two point authentication).
- One commenter suggested that court-ordered releases and guardians be scanned into an electronic medical record system.
- Commenters suggested the establishment of electronic access measure best practices through CMS or HIPAA guidance, including provisions for access in cases of incapacitation, foreign status, and legal representation.

Views on Authentication

- Commenters noted the value of a secure patient portal that only allows access to a specific patient medical record after identification confirmation.
- Commenters compared and contrasted authentication in banking to electronic healthcare records (e.g. two point authentication).
- Patients often share a user ID and password with a spouse, caretaker, or other designated individual; pharmacies allow a "family" account.
- Commenters questioned who would be responsible for a validation process and the validation key. Covered entity? Technology vendor?
- Commenters noted that there are several technical solutions that provide the ability to link accounts with explicit permissions.
- Commenters encouraged HHS favor solutions that support federated identity credentials across industries.

Views on Granularity of Access

- Commenters noted that there is a need for granular control of disclosure in order to maximize utility of VDT.
- Some questioned the need for role-based authorization systems rather than person-based authorization, despite audit requirements that support the latter.
- Commenters detailed instances in which they would want to disclose certain PHI based on relationships and the relevancy of the relationship to the individual's PHI.

- To eliminate issues related to VDT one commenter suggested printing only a defined portion of PHI.
- To the extent that Certified EHR Technology is incapable of tagging and segmenting data at a granular level, commenters noted that some health care providers will not be able to comply with VDT and state law concurrently. As a result, an "all or nothing" approach to authorizing VDT is suggested.
- Commenters recommended that patients should not have to share passwords with personal representatives in order to provide VDT access.
- Commenters also suggested that patients should be notified by simple unencrypted email or SMS when a personal representative signs in to VDT.
- Commenters also discussed assessing the ability of third parties to change or supplement PHI once they have VDT authority.