Health IT Policy Committee

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

Privacy & Security Tiger Team: Family, Friends & Personal Representative Access Recommendations

April 8, 2014

Tiger Team Members

- **Deven McGraw,** Chair, Center for Democracy & Technology
- **Micky Tripathi,** Co-Chair, Massachusetts eHealth Collaborative
- **Dixie B. Baker,** Member, Martin, Blanck, and Associates
- **Judy Faulkner,** Member, Epic Systems Corporation
- **Leslie Francis,** Member, University of Utah College of Law
- **Larry Garber,** Member, Reliant Medical Group
- **Gayle B. Harrell,** Member, Florida State House of Representatives
- **John Houston,** Member, University of Pittsburgh Medical Center, NCVHS
- **David Kotz,** Member, Dartmouth College
- **David McCallie, Jr.,** Member, Cerner Corporation
- **Wes Rishel,** Member, Gartner, Inc.
- **Kitt Winter,** Member, Social Security Administration
- **Stephania Griffin,** Ex Officio, Veterans Health Administration
- **Andrea Wilson,** Ex Officio, Veterans Health Administration

Agenda/Roadmap

- Present recommendations on Family, Friends & Personal Representative Access to the HITPC
  - Background
    - Current regulatory requirements Re: Family, Friends & Personal Representatives
    - VDT Under MU2
    - Family, Friends & Personal Representative Access: Intersection with VDT
  - Recommendations
    - Authorization of Friends/Family
    - Authorization of Personal Representatives
    - Education of Providers and Patients

Current Regulatory Requirements (1 of 3)

- 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 HIPAA Privacy Rule at §164.502(g) requires covered entities 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.

Current Regulatory Requirements (2 of 3)

- The Privacy Rule also permits (but does not require) covered entities to share PHI with family members or other persons who are involved in the individual's health care or payment for care.
  - PHI that may be disclosed is information directly relevant to their involvement with individual's care or payment.
  - Individual's have the right to object to such disclosures (and in that case, PHI may not be disclosed)
    - Note that in emergencies and other circumstances, covered entities may make reasonable inferences and act in the best interests of the individual w/respect to PHI disclosures to friends and family.

Source: §164.510(b)

Family, Friends & Personal Representative Access: Intersection with VDT (1 of 3)

- Patients will have an interest in friends and family having access to their PHI through VDT.
  - By law, patients can expressly authorize the sharing of their PHI with others.
- Legal personal representatives may have legal right to directly access a patient's PHI.
  - Under HIPAA, they stand in the shoes of the patient with respect to accessing PHI.

Family, Friends & Personal Representative Access: Intersection with VDT (2 of 3)

- Issues to resolve before VDT access granted:
  - Is the person authorized to access PHI through VDT, either due to authorization from the patient or due to legal status.
  - Identification and authentication of the individual or entity granted access (are they who they say they are)
- Education of patients and providers on rights, responsibilities, and limitations is key

Family, Friends & Personal Representative Access: Intersection with VDT (3 of 3)

- Patients may accomplish such VDT access on their own by sharing user names and passwords.
  - Although cannot control what patients will do, this is not advisable (less capability to determine who has taken action in VDT, for example). Education of patients about why this is not advisable is important.
- 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.

Recommendations

- We urge ONC to develop and disseminate the following best practices for assuring that access to adult patient VDT be extended to friends and family authorized by the patient, and, where appropriate, legal personal representatives.

Best Practices – Authorization of Friends/Family (1 of 2)

- Easiest case: patient makes request for VDT access for friend or family member
  - Can be done 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; capability to store electronically would be helpful
  - Out of band notification can be used to notify/confirm
    - Particularly important when patient request for proxy access is made remotely, or through software acting on the patient's behalf

Best Practices – Authorization of Friends/Family (2 of 2)

- Harder case: friend or family members makes request
  - Such access must be confirmed with patient, such as through out-of-band confirmation
  - If patient incapacitated –
    - HIPAA permits sharing of treatment-related information with friends or family (see background slide), but limited to only information relevant to treatment
    - Provider will need to consider whether providing access to relevant treatment information through VDT is appropriate vehicle

Best Practice – Authorization of Personal Representative

- Whether someone qualifies as a "personal representative" depends on state law. State law permutations on personal representative access make it difficult to make uniform national policy/best practice recommendations
- Providers should consider how they can adapt the processes they currently use for VDT to grant personal representative access to records.
- Capability to store documentation of personal representative status (as well as patient authorizations of access by friends/family) would be helpful.

Best Practices : Identity Proofing and Authentication

- Patient can provide credentials or directly authorize the access (for example, through VDT or by separate communication of contact information)
- Previous best practices re: identity proofing and authentication also apply here. (see backup slides)
- Also need to develop process and capability to cut off VDT access by friends, family and personal representatives due to patient change in preferences or changes in personal representative legal status.

Best Practices - Scope of VDT Access (1 of 2)

- VDT accounts may offer more than "all or nothing" access for proxies, with both respect to data content and functions that can be performed
- It is important to educate patients on whatever options are available, so they can make informed decisions about the scope of proxy access to be granted to friends/family. (In all or nothing contexts, it is particularly important to educate patients on the scope of data that will be accessible by anyone granted proxy access.)

Best Practices - Scope of VDT Access (2 of 2)

- For personal representatives, need to determine whether VDT access is limited to what the personal representative can legally access. (If not possible to do this, VDT access to personal representatives may not be grantable.)

Best Practices – Education of Providers & Patients

- ONC should disseminate best practices to providers, to enable them to establish (and turn off) proxy access to VDT accounts consistent with law and patient needs.
- Providers also should educate their patients on the risks and benefits of VDT, consistent with the HITPC's prior recommendations (see backup); such education should include risks/benefits of proxy access.

Accounting of Disclosures Recommendations

BACKUP

Previous Recommendations: Identity Proofing and Authentication (1 of 3)

- ONC should develop and disseminate best practices for identity proofing and authentication for patient access to portals (MU2 view, download, and transmit capability)
- Such best practices should be consistent with the following overarching principles
  - Protections should be commensurate with risks.
  - Approaches should offer simplicity and ease of use for patients and be consistent with what patients are willing and able to do.
  - Solutions should provide flexibility in the methods offered; ”one size does not fit all.”
  - Approaches should leverage solutions in other sectors, such as online banking.
  - Solutions should be accompanied by education that make these processes transparent to the patient.
  - Approaches taken should build to scalable solutions (e.g., greater use of voluntary secure identity providers such as those envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC)).
  - Solutions need to evolve over time as technology changes
- Additional PSTT Recommendations included out-of-band confirmation; using a different channel of communication with the individual to confirm establishment of an account or other activity.

Source: HITPC 05/03/13 Transmittal Letter:
http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_050313_pstt_recommendations.pdf

Previous Recommendations: Identity Proofing and Authentication (2 of 3)

Identity proofing…is the foundation for identify management.

- In-person identity proofing can be performed by the provider at the point of treatment, where a relationship and trust already exists.
- It is clear that in-person ID proofing provides the most protection. However, remote proofing is highly desired by some patient populations—such as, rural populations and the elderly-- and is needed to enable more patients to use patient portal accounts. Consequently, best practices for both options should be provided.
- Potential methods for remote identity proofing include the following:
  - Re-use of existing credentials.
  - Third-party, knowledge-based authentication. This approach involves verifying identity by asking the patient questions (developed by a third-party vendor) based on information about them resident in public records.
  - Verification against in-house systems. Provider entities may also verify identity using demographic matching against in-house practice management or other provider systems.
  - Use of technology. Providers could also use existing technology, such as personal computer cameras, to enable them to confirm the identity of the individual.

Source: HITPC 05/03/13 Transmittal Letter:
http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_050313_pstt_recommendations.pdf

Previous Recommendations: Identity Proofing and Authentication (3 of 3)

- ONC should strongly encourage providers to use more than user ID and password (single factor authentication) to permit patient access to portals. In addition, ONC should strongly encourage providers, at least initially, to drive toward protections analogous to those used in online banking, especially given consumers' familiarity with these practices…There are [also] easily used second factors that would build on passwords and provide greater assurance. Examples Include:
  - additional knowledge-based questions posed to the patient,
  - machine-to-machine technical controls that recognize the patient's customary device and trigger a request for additional authentication when a different device is used, and
  - emails to known addresses, phone calls, and/or letters that request confirmation that patients actually accessed their account or notify them of unusual account activity.

Source: HITPC 05/03/13 Transmittal Letter:
http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_050313_pstt_recommendations.pdf

Previous Recommendations: View and Download Best Practices (1 of 2)

- **View:** Provider guidance to patients should address the potential risks of viewing information on a public computer, viewing sensitive information on a screen that may be visible to others, or failing to properly log out after viewing.
- **Download:** At the time a patient indicates a desire to download electronic health information, providers should, at minimum, educate patients on the following three items:
  - 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.
  - 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.
  - Obtain independent confirmation that the patient wants to complete the download transaction or transactions.

Source: HITPC 08/16/11 Transmittal Letter:
http://www.healthit.gov/FACAS/sites/faca/files/HITPC_PSTT_Transmit_8162011.pdf

Previous Recommendations: View and Download Best Practices (2 of 2)

- Providers should also 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.
- Providers should also 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. Providers should also request that their view and download functionality include the capability to automatically terminate the session after a period of inactivity.
- ONC should also provide the above guidance to vendors and software developers, such as through entities conducting EHR certification.
- Providers can review the Markle Foundation policy brief, and the guidance provided to patients as part of the MyHealtheVet Blue Button and Medicare Blue Button, for examples of guidance provided to patients using view and download capabilities.

Source: HITPC 08/16/11 Transmittal Letter:
http://www.healthit.gov/FACAS/sites/faca/files/HITPC_PSTT_Transmit_8162011.pdf

Previous Recommendations: Query/Response (1 of 3)

- What supports reasonable reliance by the data holder that the requester has or will have a direct treatment relationship with the patient? (Examples not exhaustive)
  - The data holder's own knowledge or history of the requester's and patient's relationship is sufficient.
  - A data holder may have the capability to confirm a requester's direct treatment relationship with the patient within a network or integrated data system (IDS).

Source: HITPC 08/21/13 Transmittal Letter:
http://www.healthit.gov/facas/sites/faca/files/HITPC_Transmittal_08212013.pdf

Previous Recommendations: Query/Response (2 of 3)

- A network that the data holder trusts has rules providing accountability for false attestation, such as penalties against the requesting entity.
- A requester may provide some official communication of patient consent that does not conflict with expressions of patient wishes known to, or on file with, the data holder.
- There may be a known existing treatment relationship with the patient; the requester may have previously sent a query for the patient to the data holder.

Previous Recommendations: Query/Response (3 of 3)

- What supports "reasonable" reliance, by the data holder, that the requester is who they say they are? (Examples not exhaustive)
  - The use of a DIRECT certificate….When issued at the entity level, the expectation is that entities have identity proofed and authenticated individual participants as per HIPAA.
  - The requester may have membership in a network (HIO, vendor network, integrated delivery system (IDS), virtual private network (VPN), etc.) that the data holder trusts.
  - The requester is known to the data holder, such as through a pre-existing relationship.

Key Points from Public Comments (1 of 4)

- In a 2/3/2014 post on the Health IT Buzz Blog, PSTT requested comments on current practice and stakeholder concerns on authorization (proving right to access), authentication (proving identity), and granularity of access re: friends, family, & personal representative access to VDT accounts. More than 40 comments were received.

- **Views on Authorization (proving right to access)**
  - 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.

Key Points from Public Comments (2 of 4)

- **Views on Authentication (proving identity)**
  - 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.

Key Points from Public Comments (3 of 4)

- **Comments 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.

Key Points from Public Comments (4 of 4)

- **Comments on Granularity of Access (continued)**
  - 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.