Health Level Seven® International
Unlocking the Power of Health Information

An ANSI accredited standards developer

February 18, 2014

Deven McGraw, JD, MPH, LLM
Chair
Privacy and Security Tiger Team
Health IT Policy Committee
Hubert H. Humphrey Building
200 Independence Avenue SW
Washington, DC 20201

Dear Ms. McGraw:

Health Level Seven International (HL7) appreciates the opportunity to provide feedback on potential privacy and security policy issues that could arise when a family member, friend or legal designee is given access to patient information through the Certified EHR Technology “view/download/transmit” (V/D/T) capabilities.

HL7 is a not-for-profit, ANSI-accredited standards developing organization (SDO) dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. HL7's 2,300+ members represent approximately 500 organizations that comprise more than 90% of the information systems vendors serving healthcare in the US. As the global authority on standards for interoperability of health information technology, HL7 appreciates the opportunity to offer to provide our perspectives on these important issues. We would be happy to answer questions or provide further information on our response.

Sincerely,

Donald T. Mon

Charles Jaffe, MD, PhD
Chief Executive Officer
Health Level Seven International

Donald T. Mon, PhD
Board of Directors, Chair
Health Level Seven International

Personal Representatives:

Health Level Seven and HL7 are registered trademarks of Health Level Seven International. Registered in the U.S. Trademark Office.

HL7's COMMENTS

- **Are there policy issues that need further resolution regarding personal representative access to view/download/transmit accounts?**

  Policy Issue (1) Patients need to be informed and meaningfully consent to their personal representatives (PRs) having the extent of access that VDT affords.

  The extent of access to a patient's PHI is significantly increased via VDT. For some time, patients may remain accustomed to the level of access their personal representatives and friends and family members of their care team (PRs) have had in a paper-based health records environment, which is usually time limited, that is, from the time at which the patient agrees to having a PR. Patients may be comfortable in having a PR present during an encounter where the Patient can hear/see the PR's interaction with the treating provider and has knowledge of what part of the patient's medical history is being discussed. However, in the VDT environment, an appointed PR at the beginning of a serious illness, for example, would now have access to the entirety of the patient's PHI available via VDT.

  Policy Issue (2) Patients should have the ability to specify the extent of PR access to the portions of their VDT accessible medical history that the patient deems necessary for improved care coordination. This is similar to a limited power of attorney.

  If VDT access can be more granularly controlled, patients would be able to meaningfully consent to PR access for the portions of the patient's records or a specific time frame. Without granular, yet practical control, patients may be torn between maintaining their privacy and dignity by not consenting to PR access at all. If the HIPAA access for PRs and family members is not in the patient's control, patients may opt to not have any PR involved in their care, which may not result in the best health outcomes.

  We therefore suggest that a practical consent model is established that can enable patients to manage their PHI appropriately and clearly identifies how consent is managed as data moves between providers, patients, and personal representatives, and clarifies the obligations of the PR to address the concerns of PHI becoming available beyond the immediate patient-provider relationship. Furthermore this should clarify whether a PR is to be considered the same or different from the patient and if so how to enable health IT to help manage this as data is exchanged.

  Policy Issue (3) Patients should be able to specify that policies for data access and use, such as a consent directive for disclosure, remain in place. Note: This is similar to a patient establishment of a DNR order. The PR should not be able, without specific authorization, to reverse this or other policies put in place in advance with the provider for sharing of their healthcare information.

  Another Issue raised by the HIT Privacy & Security Tiger Team statement in this request for input is: "HIPAA permits covered entities to share identifiable health information relevant to a patient's care with family members or friends involved in a patient's care, unless the patient objects. It also requires covered entities to treat a "personal representative" (a person authorized under State or other applicable law to act on behalf of the individual in making healthcare related decisions) the same as they would treat the patient. For example, personal representatives have the same rights of access to medical record information as the patient would have."

Clarification is needed about the extent of discretion that covered entities have to designate a patient's PRs.

Policy Issue (4) If covered entities do in fact have the right to select a patient's PRs, then by policy, the PRs should only have access to the patient's VDT records by virtue of explicit and granular patient control of what portions of those records may be accessed by the PRs. This is very important because of the risk that a PR could exercise the patient's right to transmit the patient's records to any entity without limit.

- **How do health-care providers confirm that an individual is, in fact, a personal representative?**

  If patient's had VDT PR access consent directives, preferably using the HL7 Consent Directive CDA standard, then the patient can specify PR identifying information that the provider can use to verify the identity of the PR.   This is consistent with the view that patients have the right to set policy access by inclusion or by excluding some access to information that should not be shareable. Patient should be able to set and establish policy for whom and to what extent they wish to provide access to their VDT account.

  In addition providers should ensure that the PR is aware of any limitations preventing unauthorized actions to modify information prior to transmittal. This is required to ensure integrity of data sent on the patient's behalf.

  We defer to providers to clarify what types of documentation they require before they grant access to a portal for a PR.

Friends & Family

- **How are patients' friends and family provided with credentialed access to view/download/transmit accounts?**

  Patient PRs are typically provided credentialed access in the same manner as the patient, which should be based on HIPAA risk analysis of appropriate authentication LOA. In other words, the patients' friends, family and other PR should be identified as IT users, identity proofed, provided an account ID separate from the patient, and all PR actions taken on behalf of the patient should be audited so that the patient can determine what actions have been taken on their behalf.

- **Is this access "all or nothing," or are there more granular options? If the latter, how does this get accomplished?**

  Typically, the PR receives the same access as the patient, which may be a concern as identified above.
  As discussed in our response to the policy issues, if VDT capabilities are going to benefit a patient's care coordination, then the patient must be able to make granular access decisions or they are likely to avoid having PRs. A key consideration is that patients' ability to mask portions of their VDT accessible records from their PRs is not likely to result in patient safety issues to the extent that masking portions of a patient record from treating clinicians.

  "*All or nothing" option raises additional issues if HIPAA covered entities have discretion to designate PRs. As stated above, this may force some patients to choose between* *maintaining privacy preferences and having PRs, or even mentioning any potential PR to covered entities.*

In addition, covered entities may be leery of the potential for the perception of breach is a PR were to inappropriately access or disclose VDT PHI despite the patient's right to transmit their records to whomever they please.

The technical normative standards for accomplishing granular patient control are well-known and have been shown to be feasible in a number of ONC and FHA sponsored pilots, including: ONC Standards and Interoperability Data Segmentation for Privacy Implementation Guide and the HL7 and IHE standards version of the same; HL7 Consent Directive CDA; the HL7 Healthcare Privacy and Security Classification System; and HL7 Security Labeling Service.

These efforts are summarized below:

- *CDA Consent Directive – which enables the electronic documentation of the act of a patient consenting or authorizing some policy, with parameters captured on that instance. This CDA consent directive can also hold a policy fragment or whole policy in a standards based policy language like XACML.*
    - *This could be used to capture a patient authorizing a Personal Representative. It can be used to identify various limitations that the PR would have.*
    - *This model has been piloted successfully*
    - *This model is starting to get traction.*
    - *Without specific drivers, it will likely take some number of years of maturation before it could be mandated. On the other hand, maturity may be advanced based upon community uptake and ONC priorities (e.g., meaningful use incentives).*

- *Healthcare privacy/security Classification System (HCS) and the USA realm DS4P – a model for processing healthcare information relative to policies including consents/authorizations and relative to the requestor of data so as to provide the appropriate disclosure, thus preventing improper access.*
    - *This model has been piloted*
    - *This model has some very targeted uses*
    - *Without specific drivers it will likely take some number of years of maturation before it could be mandated. On the other hand, maturity may be advanced based upon community uptake and ONC priorities and by incorporating HCS into high priority projects such as HL7 Fast Healthcare Interoperability Resource (FHIR).*
    - *There are efforts to fold these concepts into the EHR functional model as well as FHIR.*
        - *This is a work in progress*
    - *There are efforts to define service definitions that would support these concepts*
        - *This is a work in progress.*

- *Security/Privacy Audit Logging and Reporting – This supports the recording when data is accessed, used, or disclosed (as well as other security events), such that security and privacy accountability can be shown. Specific to this use-case is that following these standards enables providing the patient with an Accounting of Disclosures. This is a report that utilizes the Security/Privacy audit log as well as other knowledge to produce*

Health Level Seven and HL7 are registered trademarks of Health Level Seven International. Registered in the U.S. Trademark Office.

a report that shows what data was disclosed to who and why. This functionality should be seen as critical to the use-case being discussed to enable the patient to understand what is happening with their data, especially regarding their PR authorizations.

  - *This is based on IHE-ATNA*
  - *This has been folded into EHR functional model*
  - *This has been folded into FHIR*
  - *This has a SOA service definition*
  - *This is in moderate use globally*
  - *More effort is needed on the reporting side*
  - *It likely is mature enough to encourage, but not mandate*

We believe that substantial efforts are in progress, but much more work is necessary to solidify these standards to support a practical consent model to manage personal representatives. In this regard, the applicable standards are not exclusive to the US realm. There is interest in the EU, and a proposed model DS4P Implementation Guide (Germany, Austria, Switzerland) has been proposed based upon the US balloted standard. These activities may encourage more rapid maturation and adoption.

Health Level Seven and HL7 are registered trademarks of Health Level Seven International. Registered in the U.S. Trademark Office.