Appendix: Health Level Seven (HL7) International Comments on Security and Privacy Aspects of the ONC Draft Trusted Exchange Framework (TEF) and the Draft U.S. Core Data for Interoperability (USCDI).

Additional Principles

The following principles are important in ensuring the security and privacy of information residing in health information networks and we recommend their addition to the TEF.

Recommend a new subsection under the Principle 4 (with appropriate numbering- we use 4.x for ease of reading for these comments) to be referenced in other places in the document as appropriate:

Principle 4.1: Persist Access Control of Health Information over its Lifecycle

Every entity participating in a Quality Health Information Network (QHIN) that controls EHI must enforce persistent access control\(^1\) over shared health information (both ePHI and eHI) throughout its lifecycle such that, at any time, and in the custody of any entity, before and after exchange, the information shared remains under enforced privacy and security protections intended by the original discloser in accordance with the applicable jurisdictional, organizational and patient privacy policies\(^2\) that governed the original disclosure.

Principle 4.2: Privacy Tag Sensitive Data with Security Labels:

Various laws and regulations require that, certain types of health information (e.g. sexual abuse, substance use disorders, HIV, mental health) are considered more sensitive and require a higher level of confidentiality protection by entities that control PHI in order to encourage individuals with these conditions to seek urgently needed treatment.

In order to achieve compliance with these requirements, every entity participating in a Quality Health Information Network (QHIN) that controls EHI must be able to:

- Assign security labels to information in their custody with standards-based privacy tags indicating the confidentiality, sensitivity, integrity, and provenance, as well as any “handling instructions”\(^3\), such as limitation on redisclosure and purpose of use as required by applicable policy.
- Ensure that the recipient entities are capable of understanding and complying with the security labels.\(^4\)

---

\(^1\) For standards related to this capability, see HL7 Version 3 Standard: Privacy, Access and Security Services (PASS); Access Control, Release 1, which describes the conceptual-level content, structure, and functional behavior of information important to healthcare access control systems, including support for enterprise to enterprise access control and patient participation in the healthcare ecosystem.

\(^2\) Patient privacy policies are stipulated by “consent directive”, and include HIPAA Notice of Privacy Practices acknowledgement, whether explicit or implicit; HIPAA Authorizations for Disclosure for coverage, research, marketing, and to third parties; consent to use and disclosure of specially protected information governed by federal or state law more stringent than HIPAA such as 42 CFR Part 2; HIPAA consent for restrictions to which a covered entity agrees or is required to uphold, such as non-disclosure to payers for services the patient paid for in full; and HIPAA Individual Right of Access “directives” submitted to covered entities.

\(^3\) Handling instructions, also known as “handling caveats” are specific rules which apply to the use and processing of a data item after its release, which are issued by the originating Entity, recorded as labels on the data, and must be honored by any recipient entity across the network. Handling instructions are an important tool in ensuring a persistent access control system across policy domains. The syntax and vocabulary for handling instruction use in healthcare are included in HL7 Healthcare Privacy and Security Classification System (HCS), Release 1.
• Enable recipient entities to hold themselves accountable via accounting of disclosures.\(^5\)

To support these expectations, the HL7 Security Working Group is authoring a Maturity Glide Path paper, expected to be published this fall, providing guidance on how entities that collect and process health information would be able to specify their capability to computably generate, consume, and enforce security labeled information based on the normative HL7 Security Labeling Service\(^6\) standard.

In addition, the HL7 Security Work Group is developing the means for run-time bridging of security labeling maturity levels among policy domains such as HINs using the HL7 Trust Framework for Federated Authorization\(^7\) based FHIR Trust Contracts.

For example, a disclosing HIN may capable of labeling of a C-CDA, a HL7 Version 2 message, or a FHIR Bundle within the message content so that end users who are authorized to access some but not all of labeled content will be permitted to access the less confidential information. If the requesting HIN is not able to support this level of access control, then policy bridging via exchange of FHIR Trust Contracts that convey coded “trust marks” as certified capability claims, would result in the disclosing HIN sharing the content with the high-water mark label in the header. As a result, the content can be compliantly shared by the discloser while the recipient HIN and/or HIN participant end users who are not authorized to access more confidential information would not be able to access any of the labeled content. Despite this impedance, policy bridging using computable privacy tag in labeled content achieves an important level of trusted cross HIN interoperability even if authorized end users would need means to share less confidential information if necessary for patient safety.

**Principle 4.3: Enforce Intended Purpose of Use:**

Based on the principle of least privilege, end users must request data only for the minimum purposes required to conduct business and HINs must:

- Label outgoing data with the intended purposes of use.
- Ensure that appropriate end user access control is enforced so that requesters will only receive information for the purposes they are authorized to receive it

Entity-specific authorized purposes can be identified in the on-boarding process based on the nature of the entity’s business and its relationships with patients are clearly aligned to uses and disclosures authorized by applicable privacy policy.

---

\(^4\) Requesters of information containing HL7 security labels, which encoded protections required under privacy laws must, at a minimum be able to computably consume, persist, and enforce the encoded policies. If they are unable to do so, then their requests should be denied especially if the recipient's inability to comply could result in a breach. Examples include the required C-CDA header confidentiality code; a HL7 Version 2 Admit, Transfer, and Discharge (ADT) message with access restriction value (ARV) segments at the PID or PV1 segment stipulating TEFCA permissible purposes of use or indicating that the patient is a VIP or has a history of opioid addiction; and security labels contained FHIR Resource meta.

\(^5\) HIPAA required Accounting of Disclosures is currently handled manually. HL7 Security Work Group is in the process of specifying how to use FHIR AuditEvent to generate computable patient friendly Accounting of Disclosures. Adoption of a standard approach for computable generation would expedite wider use of this HIPAA requirement to assert and ascertain discloser’s accountability.

\(^6\) HL7 Version 3 Standard: Privacy, Access and Security Services; Security Labeling Service, Release 1 (SLS), which specifies interoperable Security Labeling functional capabilities that are exposed through well-defined, technology agnostic service interfaces. Functional capabilities will likely include the following component services and infrastructure: - Security Labeling Manager (SLM) - Security Labeling Service (SLS) - Trust Fabric Services - Security and Privacy Ontology based terminology service - Privacy Protective Services.

\(^7\) The HL7 May 2017 Informative 2 Ballot V3 PSAF Chap 2 TF4FA Vol 1 Conceptual Model and V3 PSAF Chap 2 TF4FA Vol 2 Behavioral Model, is slated for the upcoming May 2018 ballot cycle.
Similar to a number of international bodies, the US has developed a Code of Fair Information Practices. These practices are foundational to HIPAA, Privacy Act, and FTC Fair Information Practices Principles (FIPP). A key principle in this Code is the right of information subjects to understand and agree to the purpose for which their information is used, and as a result, should not be surprised to find it used for unintended purposes.8

Under the HIPAA Privacy Rule, any use of information must be restricted to the purposes of use for which it was intended at the time of collection, access, use or disclosure. Repurposing, i.e. using information for the purpose other than what was intended, should require authorization by the originator of the information for purposes of treatment, payment, operations, and public health; and must require authorization by the patient for purposes of research, coverage determination and marketing.

In health information networks, this principle means that when data is shared with an entity, the originator must specify the set of authorized purposes of use (usually treatment, payment, operations or a subset of these, and the additional purposes included in TEFCA) as handling instructions, and the recipient must abide by these intended purposes, i.e. refrain from using data for any other purposes (repurposing) without getting reauthorization from the originating entity.

Specific Comments on the Trusted Exchange Framework:

Publish, keep current, and make publicly available the Qualified HIN’s privacy practices (p. 17). HINs and their participants should ascribe to the following privacy practices:

3. Clearly specify the minimum set of “permitted purposes” for using or disclosing ePHI or other identifiable Electronic Health Information within the TEFCA and promote limiting the use of identifiable Electronic Health Information to the minimum amount required for non-treatment purposes. If there are technical variables, the Qualified HINs should clearly specify them.

Comment: It is essential that the Trusted Exchange Framework set clear "rules of the road" about how permitted purposes are determined for specific instances of exchange, especially with respect to the how HINs construe their participants’ relationships with patients, which HIPAA requires for certain uses and disclosures. At this juncture, there may be sufficient variance to impeded cross-HIN sharing.

Some HINs may exchange patient information with other HINs based on or without concern that the recipient HINs determination about which of its participants have or have had a relationship with patient is different enough to result in sharing that was not intended by the patient or the originating provider. It may be the case when information is pushed or pulled across multiple HINs, that each downstream HIN has a different approach to making this participant/patient relationship determination.

Without transparency on how permitted purposes are determined and variance eliminated, HINs with more stringent interpretations may resist sharing with HINs that interpret patient to covered entity relationship more loosely or make a determination of such relationships using different criteria. This resistance may be prudent if the custodian HIN considers a downstream HIN's permitted purpose policies a privacy liability risk.

8 See Analysis of Privacy Principles: Making Privacy Operational v.2 2007 for an overview of international privacy frameworks’ purpose of use principles. HHS HIPAA Privacy FAQs list permissible purposes of use @ Summary of the Privacy Rule PDF - PDF.
If patient and provider expectations about the purposes for which they share information are not met, the TEFCA goals of gaining their trust will likely not be achieved.

**HL7 recommendation 1:** To evaluate the risk of disclosure for impermissible purposes, ONC should work with the RCE and other stakeholders to analyze current practices, and develop clearer guidance about how participant relationships with patients are determined to ensure that uses and disclosures are compliant with applicable privacy laws. Below are some examples of practices that risk policy impedances among HINs, and which may result in lower uptake of TEFCA.

Some HINs broadcast a patient's treatment information such as HL7® Admit, Discharge, and Transfer (ADT) messages to any covered entity that they determine has or has had a relationship with the patient. These HINs may base that determination on past HIN mediated transactions related to the patient involving the participating provider or payer. Relationship determination about participating providers or payers may also be based on feeds from health plan enrollment or claims databases.

Generally, it is not clear that payers should receive ADT notifications through a HIN. Payer should have access to treatment information based on a provider seeking payment. ADTs are disclosed for treatment purposes to coordinate of care for treatment and program eligibility, not for the broader activities associated with care coordination and case management, which could include interactions not only with payer case managers to manage costs, but with reinsurance case managers for the same reason. ADTs may include information related to coverage, but that is intended for use by providers.

In addition, we believe that providers should receive ADT notifications when they proactively list patients for whom they have a current or prospective treatment purpose to be monitoring to avoid unwarranted and perhaps unwanted proliferation of patient records, increasing the possibility of breach, or use or disclosure for impermissible purposes.⁹

**HL7 Recommendation 2:** TEFCA should ensure, consistent with our understanding of HIPAA, that if health information is disclosed by a participant through a HIN (whether via notification “push” or in response to a query) to a provider for the purpose of treatment, then that provider should not use that information for its own payment or operations purposes (including operations conducted by another covered entity which had a relationship to the patient, e.g., for population research or quality improvement activities) unless the provider actually treats the patient and generates its own record.

**HL7 Recommendation 3:** HINs may have different interpretations about whether a payer has or has had a payment relationship with a patient and timeframes in which that relationship is considered effective. A HIN that bases sharing relationships among provider and payer participants based on whether the patient was an enrollee rather than there being a claim paid for the individual may incorrectly be sharing that patient's information. For example, if an individual enrolls in a health plan, but never receives services paid for by that health plan, then the HIN would be impermissibly disclosing the individual's health information to that payer. TEFCA should address the need to ensure that the source of participant/patient relationship information is the most accurate and up-to-date.

**HL7 Recommendation 4:** Patients typically do not have insight into the list of HIN participants with which they are determined to have or have had a relationship. If the patient inadvertently discovers that the HIN has assumed this relationship exists, the patient may not have recourse to challenging disclosures to a specific participant, perhaps because the HIN does not have the technical capability of preventing further disclosures. The exception is where the patient has a legal right to authorize sharing their information via, for example, a

---

⁹ “Treatment” generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another. [HHS Provider FAQ: Uses and Disclosures for Treatment, Payment, and Health Care Operations](http://www.hhs.gov/ocr/privacy/hipaa/faq/usesdisclosurespurpose/index.html).
42 CFR Part 2 consent directive. In this case, some HINs support the patient's ability to update the list of participants which are authorized to share the patient's health information.

TEFCA should require that each QHIN and/or HIN/Participant as appropriate implement a patient friendly capability, such as a portal, so that individuals can access the list of entities authorized to share their health information when their records first become available through the HIN, and on an ongoing basis. Individuals would be able to challenge relationships that they consider incorrect, e.g., when they switch providers, the previous provider should have no need to query for or receive HIN mediated health information. This capability should also be capable of managing the patient's accounting of disclosure requests and responses.

RE: Page 17 Publish, keep current, and make publicly available the Qualified HIN's privacy practices. HINs and their participants should ascribe to the following privacy practices:

3. Qualified HINs must have the capability to document and/or capture patient consent or written authorization if required by law and communicate such consent upon request.

HL7 Recommendation: Cross HIN Approach to Harmonize Healthcare Consumer Privacy Protections:

WE recommend that ONC encourage states to harmonize privacy legislation using computable policy bridging to allow all health information to be shared in accordance with each HINs consent policies at the appropriate juncture.

- HINs that share individual health information by default, which is the majority: Continue opt-in by default to collection, access, use and disclosure of health information governed by HIPAA (recognizing that this may be a two stage authorization process for collection and sharing by some HINs), while giving all healthcare consumers continuous opportunity to opt-out in whole or part (i.e., allow restrictions use and disclosure by information type and sensitivity, purpose of use, recipients and duration.)
- HINs that share health information only if the individual explicitly agrees: Continue opt-out by default to collection, access, use and disclosure of health information governed by HIPAA (recognizing that this may be a two-stage authorization process for collection and sharing by some HINs), while giving all healthcare consumers continuous opportunity to opt-in in whole or part (i.e., allow exceptions to sharing e.g., to a specific recipient or for purpose of emergency treatment.)

The TEFCA should require that all HINs implement security labeling to distinguish sensitive conditions governed by laws preempting HIPAA (such as mental and behavioral health, HIV, sickle cell anemia, substance use disorder, sexual or relationship abuse, and minor’s health as a matter of policy) to enable cross HIN policy bridging necessary to ensure that a recipient has the capability to enforce the sender's policies.

The TEFCA should require that all HINs support the ability of healthcare consumers, whether the HIN operates under an “opt-in” or “opt-out” regime, to manage the collection, access, use, or disclosure of their health information to any recipient by information type and sensitivity, and purpose of use via their HIPAA Right of Access. This requirement includes the ability for the individual to share information labelled as additionally protected under privacy laws more stringent than HIPAA. For example, if an individual exercises HIPAA Right of Access to share Part 2 governed information with a research App, then the disclosing entity must label that information with privacy tags comporting with Part 2 disclosure requirements if the individual intends the end user to comply with that law.
Part A Detailed Comments

General. Information protected under 42 CFR Part 2, or state law that distinguishes particular information as requiring special protections, should, under a trust exchange framework, be clearly marked and identified with, at a minimum, the HL7 security classification of "Restricted". It is through this mechanism that security access and privacy requests of the patient can be honored and appropriate records of disclosure of such information maintained.

Page 19, Principle 4– Privacy, Security, and Patient Safety: Exchange Electronic Health Information securely and in a manner that promotes patient safety and ensures data integrity.

HL7 comment: re: “Exchange Electronic Health Information securely and in a manner that promotes patient safety and ensures data integrity”.

Principle 4, Subsection A. The principle lists integrity and patient matching as being important for patient safety, but makes no mention of privacy.

Security for exchanges includes mechanisms to enforce data confidentially as well as data integrity. We suggest that ONC add data confidentiality enforcement to this section.

Principle 4, Subsection B. Capture of required consent or authorization is listed as a required capability, but no mention is made for the actual enforcement of either or how restrictions on purposes of use such as the sharing of ePHI for healthcare operations only among those with a relationship with the patient is to be implemented. Simply electronically capturing patients’ permission will not engender needed trust.

Privacy would be better ensured if patients had the enforceable right to designate certain information (HIV, Substance Use Disorder (Opioid abuse) as sensitive under applicable law, requiring clinicians and other end users to have clearances for such information and training regarding their responsibilities for safeguarding such information.

We recommend that the final TEFCA provides further elaboration on QHIN requirements to enforce patient privacy required by applicable policy.

Comment:

Individuals should feel as comfortable about exercising their HIPAA right of access electronically as they do sharing portions of their hard copy designated record set. HL7 privacy tags enable individuals to share even their sensitive health information with researchers, care coordinators, and wellness Apps knowing that the privacy tagged information they disclose will inform end users about the level of confidentiality protections and purposes of use they expect for that information.

Part B Detailed Comments

Page 27: Definition of SSL. There are currently no secure versions of SSL and both v2.0 and v3.0 have been prohibited by NIST due to security vulnerabilities. SSL should not be used anymore and TLS v1.2 or 1.3 (upcoming) should be used instead.

Section 3.1.8d. It is not clear why only SAML is required here and alternatives like OpenID Connect are not mentioned.

Section 6.1.6. Providing consent can be either in the form of sending a copy of the consent or a link to it. Distributing links to a consent has the advantage of ensuring the latest version of the consent will always be referenced and in case of changes or revocation, no redundant outdated copy is maintained elsewhere.
Section 6.1.7. Since there has been an emphasis on distributing consent, it should be noted and emphasized here that revocation of a consent must also be duly distributed to ensure any parties granting access based on an old consent will get a revocation notice and update the record.

Section 6.2.3(iv). The SMART profile does not currently provide support for security labelling. The requirement for labeling should either be mentioned separately or require that the future version of SMART incorporate security labeling support.

Section 6.2.7(i). We suggest removing the paragraphs referencing substitution and transposition ciphers. These are not by any means secure cryptographic tools and add no security value over plain-text transportation. Mentioning these ciphers as if they will add any security value is misleading and gives a false sense of security for a system that uses them.

6.2.7 (ii) and (iii). These requirements should not be listed under “Transport Security”. There are all OAuth requirements and OAuth is a protocol at the application layer and not at the transport layer. These should be moved to a separate section.

6.2.7 (ii) a. It is not clear why this requirement is recommended. Arguably, supporting dynamic client registration could be contrary to having a thorough identity-proofing and onboarding process. It should be clarified that when/if this profile is supported it must be restricted to dynamic registration only by clients belonging to an entity which is already identity-proofed and on-boarded.

6.2.8. Change “SSL” to “TLS”. See comment at page 27 about SSL above.

6.2.8 (i). This section should also include a requirement for using the latest version of the TLS protocol (1.2 and the upcoming 1.3) which supports stronger cryptographic algorithms as detailed in the rest of this section and deprecates support for weak, outdated cryptographic algorithms known to be insecure (as referred in passing later in 6.2.11).

6.2.8 (ii). There are other algorithms than SHA-256 which are known to be as secure or stronger. The requirement should either state that SHA-256 is an example or use it as a minimum and allow stronger algorithms such as SHA-512.

6.2.8 (ii). Reference Certificate Authority policy requirements from in ISO 17090-1, -2, and -3.

6.2.10 (i). Security audit events: Utilize the security audit events in IHE ATNA (already cited as a security requirement) and remove the four bullets.

9.1.1. The key size 2048 is specific to public cryptography and specifically RSA. The statement in not specific enough.

10.1.1. The use of “mutually” should be clarified to include indirect (e.g. tree of trust or bridge-based) mutual trust, and not only direct mutual trust.


Although included in the eHealth Exchange DURSA purposes of use, emergency treatment is not being used or implemented for use, and as a result, emergency responders are unable to obtain urgently needed health information. This issue was made particularly clear in VA facilities during the recent devastating fires. In addition, the many recent natural disasters and multiple mass casualty events in the US make it abundantly clear that the Common Agreement must include support for differentiated purposes of use needed for
communications during to these distinct type of events given often different types of end users and the type and availability of the information needed. In fact, it might be the case that the specificity of core information needed for emergency care should be predefined, and the allowable purposes of use pre-labeled to expedite this communication.

For these reasons, HL7 [Security and CBCP WGs] strongly recommend that TEFCA implementation add the following current and proposed HL7 security label codes to allow for emergency treatment purpose of use generally, and specializations of that code to differentiate emergency treatment purpose of use for those personnel explicitly provisioned to administer emergency treatment within emergent care contexts from those end users not so provisioned and take accountability for a policy override to access information for emergent care needs, known as “break the glass”. In addition, add the current HL7 disaster purpose of use for communicating in a National or local disaster for a population. Below are the current and likely to be adopted specialization:

**HL7 Purpose of Use code DISASTER (disaster).** Definition: To perform one or more operations on information used for provision of immediately needed health care to a population of living subjects located in a disaster zone.

**HL7 Purpose of Use code ETREAT (Emergency Treatment).** Definition: To perform one or more operations on information for provision of immediately needed health care for an emergent condition

Proposed **HL7 Purpose of Use code for March 2018 Harmonization cycle:**

**HL7 Purpose of Use code ERTREAT (Emergency Room Treatment).** Definition: To perform one or more operations on information for provision of immediately needed health care for an emergent condition in an emergency room or similar emergent care context by end users provisioned for this purpose, which does not constitute as policy override as in a "Break the Glass" purpose of use.

**HL7 Purpose of Use code BTG (Break the Glass).** Definition: To perform one or more policy override operations on information for provision of immediately needed health care for an emergent condition affecting potential harm, death or patient safety by end users who are not provisioned for this purpose of use.