Health Level Seven® International
Unlocking the Power of Health Information

An ANSI accredited standards developer

`

January 14, 2018 (DRAFT)

Katie MacFarland
Applied Cybersecurity Division
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

Submitted electronically to: http://www.nist.gov/privacyframework

**Re:** Developing a Privacy Framework (NIST)

Dear Ms. MacFarland:

Health Level Seven (HL7®) International welcomes the opportunity to submit comments on the Request for Information (RFI) regarding the NIST Privacy Framework: An Enterprise Risk Management Tool ("Privacy Framework") HL7 is a not-for-profit, ANSI-accredited standards developing organization dedicated to providing a comprehensive framework and related interoperability standards, including the rapidly evolving Fast Healthcare Interoperability Resources (HL7® FHIR®), the Consolidated Clinical Document Architecture (C-CDA®), and the widely used V2 messaging standards. HL7 has more than 1,600 members from over 50 countries, including 500+ corporate members representing healthcare payers and providers, government stakeholders, pharmaceutical companies, vendors/suppliers, and consulting firms. As the global authority on interoperability in healthcare, HL7 is a critical leader and driver of standards. The products of our organization provide the underpinnings for connected, patient-centered health care and an information highway for precision medicine. It is important to note HL7 is commenting here as a Standards Setting Organization, and not one that produces personally identifiable information (PII) or products or services that collect or process PII. We want to recognize the HL7 Security Work Group who has submitted substantive feedback on relevant questions posed by NIST.

HL7 appreciates NIST's effort to better understand common privacy challenges, high-priority gaps and others issues that could be addressed through a voluntary Privacy Framework or a related roadmap. HL7 can be helpful in this regard as we are an active leader on privacy and security issues. Our firm and on-going commitment is demonstrated in HL7's standards, informative guidance materials, and privacy/security assessment tools. HL7's comments on the Privacy Framework feature detailed feedback and Appendix 1 outlines relevant HL7 privacy and security resources. Note that there are more than 20 existing HL7 educational and other resources listed for NIST to leverage.

Throughout our comments, HL7 highlights attributes that are of particular importance to include in the Privacy Framework and related development. A new privacy and security framework should be:

- Consensus-driven and developed and updated through an open, transparent process;
- Adapatable to many different organizations, technologies, lifecycle phases, sectors and uses;
- Risk-based, outcome-based, voluntary, and non-prescriptive;
- Compatible with or may be paired with other privacy approaches; and
- A living document.

HL7 also strongly recommends that the ANSI Essential Requirements, including due process and related benchmarks, be included as an anchor of standards related to the NIST Privacy Framework. These can be accessed at: https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2019_ANSI_Essential_Requirements.pdf.

As a global interoperability leader, HL7 supports NIST's effort by providing its members, especially standards developers and implementers, with a well-recognized suite of standards, informative documents, and projects for developing health information technology with privacy and security by design. HL7 stands ready to further share its cross-border expertise and perspectives by meeting with NIST and discussing our Privacy Framework recommendations. Should you have any questions about our attached comments, please contact Charles Jaffe, MD, PhD, Chief Executive Officer of Health Level Seven International at cjaffe@HL7.org or 734-677-7777. We look forward to continuing this discussion and offer our assistance to NIST.

Sincerely,

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

Calvin Beebe
Board of Directors, Chair
Health Level Seven International

# HL7 Responses to NIST RFI Questions

**Organizational Considerations: Topic 2**
**2. The greatest challenges in developing a cross-sector standards-based framework for privacy.**

HL7 possesses notable, deep and practical expertise about implementing privacy frameworks across sectors and borders. In the US, HL7 standards support HIPAA as well as non-HIPAA covered health information. As an international organization, HL7 has responsibilities to address privacy protections and mitigate privacy risks related to its own organization across multiple international privacy policy jurisdictions. For example, HL7 has recently implemented the safeguards required by the EU General Data Protection Regulation 2016/679 (GDPR) to ensure that all members are aware of its privacy and security practices in compliance with international Privacy Frameworks. Importantly, HL7 also facilitates knowledge and tools that bridge and leverage HL7 standards in support of specific Privacy Frameworks. One example is a GDPR white paper on using the Fast Healthcare Interoperability Resources (FHIR) specifications to operationalize some of the GDPR requirements, and a related implementation guide that is under development. These are available at FHIR- GDPR with background at HL7 Standards in support of computably implementing General Data Protection Regulations (GDPR) requirements for healthcare. While HL7 standards support multiple US, EU, and other policy regimes, it can be a challenge for organizations when different sectors or different jurisdictions impose different standards for the same data with the same uses or users of it. HL7 is equipped and prepared to further share its expertise on developing a cross-sector standards-based framework for privacy with NIST.

**Organizational Considerations: Topic 3**
**3. How organizations define and assess risk generally, and privacy risk specifically.**

HL7 embraces a comprehensive perspective on the protection of health information. Rather than viewing privacy and security risks in silos, HL7 cultivates an overarching Framework that encompasses both privacy and security as two sides of the same coin, essential for establishing trust. HL7 also recognizes privacy is also of key importance to safe and effective patient care. Unless patients believe that their health information will be kept private and secure, they will be less willing to share that information fully with their healthcare providers. For this reason, HL7 fosters technologies that support "sharing with protection" to enable the balancing of patient privacy and patient safety.

**Organizational Considerations: Topic 5**
**5. Current policies and procedures for managing privacy risk.**

HL7 emphasizes the importance in this topic area, of not only aligning NIST's Privacy Framework with current policy but also ensuring that the Privacy Framework complements and conforms to emerging privacy and security policy. Two important examples of emerging practice and policy at the U.S. national level are the National Telecommunications and Information Administration (NTIA) *Request for Comments on Developing the Administration's Approach to Privacy* and the U.S. Department of Health and Human Services' *Request for Information on Modifying HIPAA Rules to Improve Coordinated Care*.

**Organizational Considerations: Topic 8**
**8. The minimum set of attributes desired for the Privacy Framework, as described in the Privacy Framework Development and Attributes section of this RFI, and whether any attributes should be added, removed or clarified.**

HL7 re-affirms all seven of the minimum attributes NIST cites as necessary for its Privacy Framework to be effective. Our organization believes attributes that are of particular importance include the Privacy Framework and related development being:

- Consensus-driven and developed and updated through an open, transparent process;
- Able to be adapted to many different organizations, technologies, lifecycle phases, sectors and uses;
- Risk-based, outcome-based, voluntary and non-prescriptive;

- Compatible with or may be paired with other privacy approaches; and
- A living document.

HL7 also strongly recommends that the ANSI Essential Requirements, due process and related benchmarks anchor the NIST Privacy Framework. More information about the ANSI Essential Requirements can be found at: https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2019_ANSI_Essential_Requirements.pdf.

**Organizational Considerations: Topic 14**
**14. The international implications of a Privacy Framework on global business or policymaking in other countries.**

At the intersection of Privacy Frameworks and policy HL7 as an SDO is prepared to offer assessment tools and implementation standards to aid the national and international healthcare community in establishing, adopting, or complying with appropriate Privacy and Security Frameworks and to enable the bridging of those frameworks. As an international SDO, HL7 is fully aware of, and our standards support, the several well-recognized global privacy frameworks. Our organization takes a policy agnostic position on the adoption of any one Privacy Framework. Regarding jurisdictionally adopted privacy frameworks, HL7 notes that they evolve as their policy domains do. HL7 supports a NIST Privacy Framework that provides guidance and tooling, enabling any policy domain to adopt interoperable standards so that each policy domain can adopt a context appropriate set of assessment tools, preferably with policy bridging capabilities.

**Structuring the Privacy Framework: Topic 18c**
**18. Please describe your preferred organizational construct for the Privacy Framework. For example, would you like to see a Privacy Framework that is structured around:**
**c. The NIST privacy engineering objectives of predictability, manageability, and disassociability or other objectives;**

**Disassociability** - NIST notes in Privacy Framework RFI-related documents, "disassociability captures one of the elements of privacy-preserving systems—that the system actively protects or "blinds" an individual's identity or associated activities from exposure. Unlike confidentiality, which is focused on preventing unauthorized access to information, disassociability recognizes that privacy risks can result from exposures even within an authorized perimeter. Disassociability advances the capabilities of a privacy-preserving system by engaging system designers and engineers in a deliberate consideration of points of exposure that are not essential for the operation of the system. Many cryptographic techniques that exist today or are currently being researched could be mapped to disassociability. Adopting disassociability as an objective could raise awareness of the benefits of these techniques and increase demand for more advances. A further consideration is whether a taxonomy could be constructed of existing identity-related classifications, including anonymity, de-identification, unlinkability, unobservability, pseudonymity or others. Such a taxonomy could potentially support more precise control mapping and risk mitigation."

HL7 does have a section in its FHIR specification relevant to disassociability that addresses the issues above. It can be found at: http://build.fhir.org/secpriv-module.html#deId. The full text of this FHIR specification is also below.

(http://build.fhir.org/secpriv-module.html#deId)
6.0.5.8 De-Identification, pseudonymization, anonymization
De-Identification is inclusive of pseudonymization and anonymization; which are the processes of reducing privacy risk by eliminating and modifying data elements to meet a targeted use-case.

Use-Case: "Requesting Client should have access to De-Identified data only."

*Trigger:* Based on an Access Control decision that results in a permit with an Obligation to De-Identify, the Results delivered to the Requesting Client would be de-identified.

*Consideration:* This assumes the system knows the type and intensity of the de-identification algorithm, where de-identification is best viewed as a process, not an algorithm - a process that reduces Privacy risk while enabling a targeted and authorized use-case.

*Modifying an element:* The de-identification process may determine that specific elements need to be modified to lower privacy risk. Some methods of modifying are: eliminating the element, setting to a static value (e.g. "removed"), fuzzing (e.g. adjusting by some random value), masking (e.g. encryption), pseudonym (e.g. replace with an alias), etc. Narrative and Attachment elements present particularly difficult challenges. See standards below for further details.

*Discussion:* Obviously the most important elements for de-identification are names and identifiers. FHIR resources have many different types of ids and identifiers that serve different purposes. Some (ids) are the basis for internal links between different resources, while identifiers are mainly - but not exclusively - for correlating with external data sources. Strategies for de-identification need to consider whether re-identification with the source system is a problem, in which case ids will need to be modified - and consistently across the resource set being de-identified. External identifiers will mostly need to be removed, but even then, where they are used for internal references within the resource set, they'll need to be changed consistently.

*Security-label:* The resulting Resource should be marked with security-label to indicate that it has been de-identified. This would assure that downstream use doesn't mistake this Resource as representing full fidelity. These security-labels come from the Security Integrity Observation ValueSet. Some useful security-tag vocabulary: ANONYED, MASKED, PSEUDED, REDACTED

Further non-HL7 dissaociability standards can be found at:
ISO 25237:2017 Health informatics -- Pseudonymization
NIST IR 8053 - De-Identification of Personal Information
IHE De-Identification Handbook
DICOM (Part 15, Chapter E)

## Appendix 1: HL7 Privacy/Security Standards and Projects Relevant to NIST Privacy Framework

The following are HL7 specifications and healthcare privacy related projects intended to support healthcare standards developers and implementers in achieving the objectives of an overarching Privacy Framework as envisioned by the NIST. The resources below also relate to:

Organizational Considerations: Topic 10
10. What standards, frameworks, models, methodologies, tools, guidelines, and best practices and principles organizations are aware of or using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels, and whether any of them currently meet the minimum attributes above.

**HL7 Privacy and Security Standards (Informative Documents)**

HL7 Standards Privacy Impact Assessment (SPIA) Cookbook - Guides HL7 standards developers through a 10-step privacy-related process for development of an HL7 standard, reducing the need to retrospectively incorporate privacy in a standard. A Standards Privacy Assessment (SPA) is a methodology assessing the possible privacy impact(s) of a Standard Under Review (SUR). It takes into account applicable privacy principles and associated privacy safeguarding requirements in order to assess the potential threats arising from the SUR that require mitigation by introducing privacy safeguards or controls. In addition, the SPA process is intended to help create information that should be used in analyzing the potential harm towards an individual that could be caused by the technology defined by the SUR.

HL7 Standards Privacy Assessment Project

Security Risk Assessment Cookbook - Instructions for HL7 standards authors and workgroup members. This Security Risk Assessment Cookbook is intended to enable HL7 domain committees and working groups to publish standards that have taken privacy and security considerations into account. This guide introduces security risk assessments and a process to facilitate completing a security risk assessment for a specific standard. Using this process will facilitate the identification of gaps in a standard's baseline security and privacy, allowing the working group to either update the standard on their own or to send a request to the Security Working Group for assistance in filling the gap. This will lead to standards that include privacy and security as part of their base, reducing the need to "bolt" security on later. As a result, the HL7 standards will better support patient safety and improved patient outcomes.

EHR Functional Model, Release 1 - The EHR functional model includes a comprehensive set of security and privacy functions. This catalog includes detailed system level requirements that are actionable and testable. Profiles of this functional model are available for many functional systems including an EMR and PHR.

HL7 Healthcare Privacy and Security Classification System (HCS), Release 1 - Foundational HL7 Privacy and Security Vocabulary used as metadata for encoding data subject, organizational, and jurisdictional privacy policies, which can be computably enforced, exchanged in an interoperable way, and supports cross-domain privacy policy bridging.

HL7 Version 3 Standard: Privacy, Access and Security Services; Security Labeling Service, Release 1 (SLS - Conceptual Behavioral Model describing how to apply and enforce security labels valued with HCS codes.

HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 - ONC optional certification standard for applying machine readable security labels, which encode data subject, organizational, and jurisdictional privacy policies, to HL7 CDA artifacts.

HL7 Version 3 Standard: Security and Privacy Ontology, (SPO) Release 1 - Formally names and describes key interrelated security and privacy concepts within the scope of Healthcare Information Technology, including security policies, and data subject, organizational, and jurisdictional privacy policies, for intra- and inter-enterprise enforcement and accountability via trust frameworks, access control, audit, and provenance.

HL7 Version 3 Standard: Healthcare (Security and Privacy) Access Control Catalog, Release 3 - Conceptual model viewpoints associated with the business requirements that relate to the content, structure, and functional behavior of information important to the Access Control area of the Privacy, Access, and Security domains within the healthcare environment.

Role-Based Access Control Permission Catalog (RBAC), Release 2 - This vocabulary enables communication of users' permissions in an interoperable way. This vocabulary can be used at a multitude of points in the Privacy and Security system.

HL7 CDA® R2 Implementation Guide: Privacy Consent Directives, Release 1 - This CDA document object captures the patient privacy preferences, authorizations, and consents. This document is used as evidence of a patient consent ceremony as well as triggers privacy policy engines to enforce the patient privacy. This is a structured document specification to exchange signed Consent Directives, and provides a computable representation of a consent directive but the resulting structured documents could be used to generate enforceable assertions or rules (e.g. SAML, XACML).

HL7 CDA® R2 Implementation Guide: Patient-Friendly Language for Consumer User-Interfaces, Release 1 - Relevant to request for Common and accessible language.

HL7 Version 3 Domain Analysis Model: Medical Records; Composite Privacy Consent Directive - HL7 Draft Standard for Trial Use Release 2 February 2010 This model contains the analysis of several representative use cases illustrating the

use of electronic privacy policies (Privacy Policy) and electronic consent directive (Consent Directive) as it relates to the Privacy Policy. This analysis provides a "composite" view of Consent Directive and their underlying privacy policies.

The SMART Application Launch Framework Implementation Guide Release 1.0.0 – This provides specific implementation guidance to secure FHIR APIs with appropriate authentication and authorization protocols. (http://hl7.org/fhir/smart-app-launch/scopes-and-launch-context/index.html)

FHIR Consent Resource - A record of a healthcare consumer's choices, which permits or denies identified recipient(s) or recipient role(s) to perform one or more actions within a given policy context, for specific purposes and periods of time.

FHIR Contract Resource - Legally enforceable, formally recorded unilateral or bilateral directive i.e., a policy or agreement.

FHIR Provenance Resource - Provenance statement indicating clinical significance in terms of confidence in authenticity, reliability, and trustworthiness, integrity, and stage in lifecycle, all of which may impact security, privacy, and trust policies.

FHIR AuditEvent Resource - The content of an AuditEvent is intended for use by security system administrators, security and privacy information managers, and records management personnel. This FHIR Resource is useful for deriving provenance and accounting of disclosure records.

7.10.1 Implementer's Safety Check List - Due to the nature of healthcare, and healthcare processes, and cultural concerns, there are a number of features in FHIR that implementers are obliged to consider in order to implement safe systems. This section is a checklist to help implementers be sure that they've considered all the parts of FHIR that could have an impact on their system design with regard to safety. Note that for this list, safety is interpreted broadly, and this check list covers security and privacy issues as well.

FHIR De-Identification, pseudonymization, anonymization - Emerging HL7 privacy-related specifications, all of which are slated to be published as ANSI recognized standards in 2019:

(In-development, not yet Available)
HL7 Trust Framework for Federated Authorization Conceptual and Behavioral Models - A general architecture for creating a trusted relationship with a healthcare partner supporting policy negotiation for security and privacy.

HL7 Provenance Conceptual Model - Conceptual-level viewpoints associated with business requirements that relate to the content and structure of provenance data, and the functional behavior of systems that manage that data, which are important to establishing the trustworthiness of specific resources within the healthcare environment.

**HL7 Privacy Projects:**

HL7 Standards in support of computably implementing General Data Protection Regulations (GDPR) requirements for healthcare.

Is Privacy Obsolete Study Group - A "crowd sourced" study of international issues related to privacy and technology. It re-affirms NIST's recent statement that the hidden burden of data breach costs has been delegated on the users.

HL7 Standards Privacy Assessment Project

**Additional Privacy and Security Projects to which HL7 Contributes:**

OASIS Privacy by Design

OASIS Privacy Management Reference Model and Methodology (PMRM) Version 1.0 Committee Specification Draft 01 26 March 2012

Privacy by Design Documentation for Software Engineers Version 1.0 DRAFT Committee Specification 02 Working Draft 08 Updated 11 January 2016

PbD-SE Conformance Maturity Model (PbD-CMM) Organizations may determine and report how mature their PbD-SE specification conformance is on a scale of 1 to 6 with conformance levels ranging from ad-hoc (1) to verifiable (6). Each higher level presupposes that all the documentation requirements in lower levels have been met and surpassed. Level 1 is the lowest level of PbD-SE maturity. The PbD-SE Conformance Maturity Model assumes continuous improvement at each level. It requires demonstration of accountability around privacy management to stakeholders as organizations climb the maturity model from Levels 1 to 6.

Participation as HL7 SMEs in the ONC Patient Choice
Project http://wiki.hl7.org/index.php?title=HIMSS_2017_Patient_Choice

ISO/IEC 29100:2011: Information technology -- Security techniques -- Privacy Framework
(https://www.iso.org/standard/45123.html)

ISO/IEC 29101:2018: Information technology -- Security Techniques -- Privacy Architecture Framework
(https://www.iso.org/standard/75293.html)

ISO/IEC 20889:2018: Privacy Enhancing Data De-identification Terminology and Classification of Techniques
(https://www.iso.org/standard/69373.html)

ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management -- Requirements and Guidelines
(https://www.iso.org/standard/71670.html)

CNIL Privacy Impact Assessment
https://www.cnil.fr/en/privacy-impact-assessment-pia

PRIPARE Handbook: Methodological Tools to Implement Privacy and Foster Compliance with the GDPR
http://prepareproject.eu/