33 West Monroe St, Suite 1700
Chicago, IL 60603-5616
Tel 312 664 4467
Fax 312 664 6143
www.himss.org

The Healthcare Information and Management Systems Society (HIMSS) is pleased to submit these comments for consideration by ONC to update the Interoperability Standards Advisory (ISA). These comments are one set in a series of comments that HIMSS has provided on the content in the new web-based version of the ISA. For more information on previous comments, please visit the HIMSS website.

Please find comments below as related to specific questions outlined in the ISA's Section VI.

In Questions 3-7 of Section VI, ONC requests feedback on the six characteristics for the standards listed in the Interoperability Needs throughout the ISA. Below is feedback HIMSS has provided on characteristics for some of the Interoperability Needs and related standards. The following comments are recommendations for information to include for Limitations/Dependencies/Preconditions and/or Applicable Value Sets for a variety of Interoperability Needs.

Feedback on I-A: Representing Patient Allergies and Intolerances; Environmental Substances: ONC requested feedback on the adoption level of Unique Ingredient Identifier (UNII) for this Interoperability Need. HIMSS suggests assigning an adoption level of 4 as seen on the representation of Food Substances Interoperability Need. UNII has been included in specifications since HITSP and is listed in C-CDA as an option for representing substances.

Feedback on I-F: Representing Imaging Diagnostics, Interventions and Procedures: For Applicable Value Sets, HIMSS suggests the creation of procedure-specific value sets for LOINC, organized by domains, to be included in this section.

Feedback on I-O: Representing Medical Procedures Performed: HIMSS suggests the creation of procedure-specific value sets for SNOMED CT codes.

Feedback on I-U: Defining a Globally Unique Device Identifier: HIMSS does not believe that an identifier such as UDI needs a value set or starter set. For example, the National Provider Identifier (NPI) or individual person identifiers of various kinds (SSN, Drivers License) do not use value sets.

Feedback on II-B: Domain or Disease-Specific Care Plan Standards: For C-CDA 2.1 in general, HIMSS suggests an adoption level of 3. This standard is required in certification, Meaningful Use Stage 3 and MACRA. However, not all EHRs are capable of meeting this requirement to date. Specifically the C-CDA Care Plan Document likely has a lower adoption for either 1 or 2, since it is a newer document type with fewer implementations. HIMSS also recommends the addition of the following clarifying text to the Limitations/Dependencies/Preconditions: "The Personal Advance Care Plan Document is for the domain of patient-authored goals, priorities and preferences, including but not limited to Advance Directives."

Feedback on II-F: Establishing the Authenticity, Reliability, and Trustworthiness of Content Between Trading Partners: HIMSS suggests adding the HL7® FHIR® Provenance Resource as an emerging standard to this Interoperability Need, since it is a Standard for Trial Use and is at FHIR® maturity level 3. This resource leverages the W3C Provenance specification to represent HL7® support of provenance throughout its standards. It is explicitly modeled as functional capabilities in ISO/HL7 10781 EHR System Functional Model Release 2 and ISO 21089 Trusted End-to-End Information Flows. Mappings are provided within this Resource.

Feedback on II-U: Support a Transition of Care or Referral to Another Health Care Provider: In response to ONC's request for feedback on "Applicable Security Patterns", HIMSS does not believe any

"applicable security patterns" need to be assigned to content standards like C-CDA, as they would vary depending on how the document is transmitted or shared. For example, the patterns would be different if C-CDA is pushed via Direct, or downloaded by a patient through a portal, or queried using an IHE document registry/repository. A security pattern makes more sense listed for the Services such as III-A "Push Exchange", which ONC already includes.

The following feedback is related to Section VI's question on sources included in Appendix I, listed below.

16. Are there other authoritative sources for Security Standards that should be included in Appendix I?

Before discussing the sources included for the security standards within the ISA, HIMSS believes greater organization of this Appendix would significantly increase the value of the information included in this section. The current sources, while incredibly important, lack any clear delineation as to how they should be leveraged. Some method of categorization should be added to the Appendix, defining the purposes for the sources included. The NIST Cybersecurity Framework provides categories for the standards included within that document (specifically in Tables 2 and 3). HIMSS suggests that ONC review this Table for potential options to better organize Appendix I.

For the sources included in the Appendix, HIMSS has identified some opportunities to expand and update the current list. HIMSS would first like to prioritize the following sources as we believe their inclusion is important to addressing the health IT security landscape.

- *NIST Cybersecurity Framework, Version 1.1: https://www.nist.gov/cyberframework/draft-version-11*
    - While HIMSS recognizes that this is a Draft version of the Framework, Version 1.0 currently listed in the ISA, this Draft version provides a lot more detail on the standards and their implementation than Version 1.0.
- *US-CERT. Information Sharing Specifications for Cybersecurity https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity* :
- *HIPAA (Version 5010) Transactions. X12 EDI Transaction Sets. See X12N (Insurance)* http://www.x12.org/x12org/docs/editransactions.pdf
    - These are basic HIPAA transactions that are essential to reimbursement. These may be outside of the scope of ISA, with its focus on clinical uses of interoperability. However, if categorization is introduced into Appendix I, this source could be listed as an additional source for consideration for administrative purposes.
- The FDA has documents on Cybersecurity Guidance that should be considered for this Appendix.
    - FDA: "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff", October 2, 2014, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf
    - FDA: "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff", December 28, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

HIMSS would also like to suggest the inclusion of the following sources.

- AAMI TIR57: Principles for medical device security—Risk management
- ASTM E1869-04:2014 Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records
- ASTM E-31. https://www.astm.org/COMMIT/E31standardseducation.pdf
- ONC Guide Privacy and Security of Health Information: https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (second edition) http://www.iso27001security.com/html/27002.html
- HITRUST Common Security Framework: https://hitrustalliance.net/content/uploads/2014/05/HITRUSTCSF-2014-v6_0-Executive-Summary-and-Introduction-FINAL.pdf
- Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
- ISO 13485 FDA's Unique Device Identification UDI
- ISO 14971: Medical devices -- Application of risk management to medical devices
- ISO/AWI 81001 Health software and health IT systems safety, effectiveness and security
- ISO/TR 11633 Health informatics -- Information security management for remote maintenance of medical devices and medical information systems
- ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002
- ISO 20429 Principles and guidelines for protection of PHI (working draft)
- ISO/IEEE 11073 "Personal Health Data (PHD) Standards"
- IEEE: "Building Code for Medical Device Software Security"
- IEC 62304: Medical device software -- Software life cycle processes
- IEC/FDIS 82304-1 "Health software - Part 1: General requirements for product safety"
- NIST Special Publication 800-185. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-185.pdf
- NIST Special Publication 800-188 (2nd DRAFT). De-Identifying Government Datasets. http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft2.pdf
- NIST Special Publication 800-184. Guide for Cybersecurity Event Recovery. http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft2.pdf
- NIST Special Publication 1800-4c. Mobile Device Security. https://nccoe.nist.gov/publication/draft/1800-4c/#t=MDSHowTo%2FCover%2FCover.htm
- NIST Special Publication 1800-8C. Securing Wireless Infusion Pumps In Healthcare Delivery Organization. https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8c-draft.pdf
- NIST Special Publication 1800-3c. Attribute Based Access Control. September 2015 https://nccoe.nist.gov/sites/default/files/library/sp1800/abac-nist-sp1800-3c-draft.pdf
- NIST Special Publication 800-121 Revision 2. Guide to Bluetooth Security. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf
- NIST Special Publication 800-178. A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). November 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-178.pdf
- NIST Special Publication 800-66 "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
- NISTIR 7497, Security Architecture Design Process for Health Information Exchanges (HIEs) (September 2010) https://www.nist.gov/healthcare/security/health-information-exchange-hie-security-architecture

- IEC 80001 series:
    - IEC 80001-1:2010 “Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities”
    - IEC/TR 80001-2-1:2012 “Application of risk management for IT-networks incorporating medical devices -- Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples”
    - IEC/TR 80001-2-2:2012 “Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls”
    - IEC/TR 80001-2-3:2012 “Application of risk management for IT-networks incorporating medical devices -- Part 2-3: Guidance for wireless networks”
    - IEC/TR 80001-2-4:2012 “Application of risk management for IT-networks incorporating medical devices -- Part 2-4: General implementation guidance for Healthcare Delivery Organizations”
    - IEC/TR 80001-2-5:2014 “Application of risk management for IT-networks incorporating medical devices -- Part 2-5: Application guidance -- Guidance for distributed alarm systems”
    - ISO/TR 80001-2-6:2014 “Application of risk management for IT-networks incorporating medical devices -- Part 2-6: Application guidance -- Guidance for responsibility agreements”
    - ISO/TR 80001-2-7:2015 “Application of risk management for IT-networks incorporating medical devices -- Application guidance -- Part 2-7: Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1”
    - IEC/DTR 80001-2-8 “Application of risk management for IT-networks incorporating medical devices -- Part 2-8: Application guidance -- Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2”
    - IEC/NP TR 80001-2-9 “Application of risk management for IT-networks incorporating medical devices -- Part 2-9: Application guidance -- Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities”

- The following NIST documents provide standards and best practices for general security areas.
    - NIST SP 800-12, An Introduction to Information Security
    - NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
    - NIST SP 800-37 “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
    - NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
    - NIST SP 800-40, Guide to Enterprise Patch Management Technologies
    - NIST SP 800-41, Guidelines on Firewalls and Firewall Policy
    - NIST SP 800-64, Security Considerations in the System Development Life Cycle
    - NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process
    - NIST SP 800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
    - NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
    - NIST SP 800-88 Guidelines for Media Sanitization
    - NIST SP 800-94, DRAFT Guide to Intrusion Detection and Prevention Systems (IDPS)

    - NIST SP 800-100, Information Security Handbook: A Guide for Managers
    - NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
    - NIST SP 800-154, DRAFT Guide to Data-Centric System Threat Modeling
    - NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- The following documents provide important guidance on Vulnerability, Threat and Incident Management.
    - NIST SP 800-51, Guide to Using Vulnerability Naming Schemes
    - NIST 800-61 Computer Security Incident Handling Guide
    - NIST SP 800-83, Guide to Malware Incident Prevention and Handling
    - NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
    - NIST Special Publication 800-150.Guide to Cyber Threat Information Sharing. October 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
    - NIST SP 800-184, DRAFT Guide for Cybersecurity Event Recovery
- The following documents provide guidance on encryption and key management.
    - NIST SP 800-57 Recommendation for Key Management
    - NIST SP 800-113, Guide to SSL VPNs
- The following documents provide guidance for workforce development.
    - NIST SP 800-50, Building an Information Technology Security Awareness and Training Program
    - Draft NIST SP 800-181 "NICE Cybersecurity Workforce Framework (NCWF), National Initiative for Cybersecurity Education (NICE)", http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf
- This NIST guidance document is not a standard but it addresses something government agencies, NIST included, have been researching for the past five years. Lightweight cryptography has applications for mobile devices, Internet of Things, and other devices/computers with limited processing power. http://csrc.nist.gov/publications/nistbul/itlbul2017-06.pdf
- With the increased adoption of HL7® FHIR® and APIs by the industry, we would also suggest inclusion of the following standards:
    - IHE – Internet User Authorization (IUA): This security profile is used with HTTP REST and leveraged in all IHE FHIR® profiles. http://wiki.ihe.net/index.php/Internet_User_Authorization
    - SMART on FHIR® also offers stricter security architecture.
    - The HEART Working Group: This initiative by the OAuth community has developed privacy and security specifications that enable an individual to control the authorization of access to RESTful health-related data sharing APIs, and to facilitate the development of interoperable implementations of these specifications by others.

Furthermore, we recommend ensuring the sources included reflect the most up to date and streamlined information. See below for suggested edits.

- NIST Special Publication: 800-63-2. Electronic Authentication Guideline. August 2013 should be removed and replaced with NIST Digital Authentication Guideline, Special Publication 800-63-3.
- NIST 800-53 is listed twice. One iteration should be removed to streamline the list.

- The language “HIPAA Security regulations that are specific to healthcare” seems to be a redundant statement as HIPAA, by definition, is specific to healthcare. HIMSS suggests adjusting the language to “HIPAA Security Rule and Tools”.
- The reference and link to NIST 1800-a-e “Securing Electronic Health Records on Mobile Devices” is incorrect, the correct title should read: NIST 1800-1 “DRAFT Securing Electronic Health Records on Mobile Devices” with the link to: http://csrc.nist.gov/publications/PubsDrafts.html#SP-1800-1