2019 Interoperability Standards Advisory

Office of the National Coordinator for Health IT

Reference Edition

Table of Contents

The 2019 Interoperability Standards Advisory represents the Office of the National Coordinator for Health Information Technology's current assessment of the heath IT standards landscape. It is for informational purposes only. It is non-binding and does not create nor confer any rights or obligations for or on any person or entity.

This document contains numerous links to other federal agencies and to private organizations. You are subject to these sites' privacy policies when you access them. HHS is not responsible for Section 508 compliance (accessibility) on other federal or private sites. HHS is not responsible for the contents of any "off-site" web page referenced from this document.

Introduction to the 2019 Interoperability Standards Advisory

The Interoperability Standards Advisory (ISA) process represents the model by which the Office of the National Coordinator for Health Information Technology (ONC) will coordinate the identification, assessment, and public awareness of interoperability standards and implementation specifications that can be used by the healthcare industry to address specific interoperability needs including, but not limited to, interoperability for clinical, public health, research and administrative purposes. ONC encourages all stakeholders to implement and use the standards and implementation specifications identified in the ISA as applicable to the specific interoperability needs they seek to address. Furthermore, ONC encourages further pilot testing and industry experience to be sought with respect to standards and implementation specifications identified as "emerging" in the ISA.

The 2019 Reference Edition ISA reflects the numerous changes made across the ISA throughout 2018. To learn more about what has changed, refer to the Recent ISA Updates page, which provides a summary of major changes to the ISA. In addition, registered users may subscribe to change notifications to be alerted by e-mail of all revisions to individual interoperability needs or for ISA-wide changes. Anyone may become a registered user, by submitting an account request. Once logged in, look for the blue "change notification" button at the bottom of the interoperability need page, or at the bottom of the home page to be notified of any changes across the ISA. An RSS feed, capturing more granular changes to individual pages, was also added in 2018.

For additional information about the ISA, including scope, purpose, structure, and an overview of the informative characteristics attributed to each standard/implementation specification, please see the Introduction text located at www.healthit.gov/isa

Section I: Vocabulary/Code Set/Terminology Standards and Implementation Specifications

Allergies and Intolerances

Interoperability Need: Representing Patient Allergic Reactions

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●●●○○	No	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	●●●●○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• SNOMED CT® may not be sufficient to differentiate between an allergy or adverse reaction, or the level of severity. • For use of SNOMED CT®, codes should generally be chosen from the Clinical finding axis. • See LOINC projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• 'Adverse Clinical Reaction' value set (OID: 2.16.840.1.113883.3.2074.1.1.30) contains SNOMED CT findings and disorders resulting from reactions to substances • 'Allergy and Intolerance Type' value set (OID: 2.16.840.1.113883.3.88.12.3221.6.2) contains SNOMED CT disorders representing classes of reactions and intolerances

Interoperability Need: Representing Patient Allergies and Intolerances; Environmental Substances

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	SNOMED CT®	Final	Production	●●●○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):

• Feedback is requested as to the extent the suggested value sets using SNOMED CT parent and child codes for environmental allergens are sufficient to meet the needs for starter value set.	• Allergic disposition (disorder) (SNOMEDCT 609328004) is parent code to:
	  ○ Environmental allergy (disorder) (SNOMEDCT 426232007)
	  ○ Allergy to substance (disorder) (SNOMED CT 419199007) and other related codes

Interoperability Need: Representing Patient Allergies and Intolerances; Food Substances

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	SNOMED CT®	Final	Production	●●●●○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):

• Feedback is requested as to the extent the suggested value sets using SNOMED CT parent and child codes for food allergens are sufficient to meet the needs for starter value set.	• Adverse Clinical Reaction (2.16.840.1.113883.3.2074.1.1.30) (SNOMED CT® disorder and finding value set)
	• Propensity to adverse reactions to food (disorder) (SNOMEDCT 418471000) is parent SNOMEDCT code to:
	  ○ Food allergy (disorder) (SNOMEDCT 414285001)
	  ○ Food intolerance (disorder) (SNOMEDCT 235719002)
	• Food Allergen (2.16.840.1.113762.1.4.1156.1) (SNOMED CT® disorder and finding value set-Steward Partners Healthcare)
	• Common dietary substances for allergy and intolerance documentation (2.16.840.1.113762.1.4.1186.3) (SNOMED CT® disorder and finding value set-Steward HL7 Patient Care Work Group)

Interoperability Need: Representing Patient Allergies and Intolerances; Medications

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	RxNorm	Final	Production	●●●●○	Yes	Free	N/A
Standard	SNOMED CT®	Final	Production	●●●○○	No	Free	N/A
Emerging Standard	*Medication Reference Terminology (MED-RT)*	*In Development*	*Pilot*	*Feedback Requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):

• When a medication allergy necessitates capture by medication class, SNOMED CT® should be used.
• MED-RT is meant to replace the VA's NDF-RT with is being sunsetted in 2018. It has the capability to represent medication classes for use as an allergen category, and currently requires MeSH terms for medication classes.
• RxNorm: Refers to the RxNorm source specifically (and not to other sources that are included with the RxNorm download).
	• Representing Medication
	  ○ Clinical Drug Ingredient (2.16.840.1.113762.1.4.1010.7) (RxNorm ingredient codes)
	  ○ Pharmaceutical / biologic product (product) (SNOMED CT 373873005) is parent to pharmaceutical/biologic classes
	• Representing Adverse Reactions/Intolerances
	  ○ Propensity to adverse reactions to drug (disorder) (SNOMED CT 419511003) is parent to:
	  ▪ Drug Allergy (disorder) (SNOMED CT 416098002) and child terms/codes

Emergency Medical Services

Interoperability Need: Representing Health Care Data for Emergency Medical Services

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NEMSIS Version 3	Final	Production	Feedback Requested	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The National Emergency Medical Services Information System (NEMSIS) administered by the National Highway Traffic Safety Administration's Office of Emergency Medical Services provides a universal standard for the collection and transmission of emergency medical services (EMS) operations and patient care data. Using NEMSIS-compliant electronic patient care record (ePCR) software products, data is collected by EMS practitioners at the point of care and includes information on the EMS system response, scene characteristics, patient demographics, patient condition, medical treatment provided, transport decision, patient and incident disposition and EMS system times (e.g., response time, scene time, transport time). NEMSIS includes the National EMS Database which accepts EMS data voluntarily submitted by U.S. States and Territories. Using NEMSIS-compliant ePCR software products, local EMS systems collect a national set of data elements for submission to the National EMS Database through their respective state. Local EMS systems and states have the option to collect additional NEMSIS data elements to meet local and state needs. The NEMSIS standard follows a 5-year revisioning cycle. The two most recent NEMSIS standard versions (V3.3.4 and 3.4.0 as of January 2018) are available for ePCR software product compliance testing and submission to the National EMS Database. NEMSIS standard version 3.5.0 is planned for release in September 2019. NEMSIS Version 3 standards (i.e., V3.3.4, 3.4.0, and V3.5.0) include integration of several HL7 data standards, such as LOINC, RxNorm, and ICD-10-CM. NEMSIS standard versions V3.3.4 and V3.4.0 are HL7 compliant and ANSI accredited. • NEMSIS uses Extensible Markup Language (XML) to move data. States and software companies create products that are used to send and receive EMS data in the proper XML format from agencies to states, then on to the National EMS Database. More information about NEMSIS is available at https://nemsis.org/technical-resources/ • Mapping and translation resources are available for mapping or translating older versions of the dataset to newer versions of the dataset.	

Encounter Diagnosis

Interoperability Need: Representing Patient Dental Encounter Diagnosis							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	SNODENT	Final	Production	●●●●○	No	$	N/A
Standard	ICD-10 Dental Diagnosis Codes	Final	Production	●●●●○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Code System**:
• SNODENT is owned, maintained and distributed by the American Dental Association (ADA). The SNODENT code set is available under license at no cost for non commercial use. The license agreement terms also permit licensees to use SNODENT in the development of non-commercial, academic, scholarly articles and presentations for publication.	• OID 2.16.840.1.113883.3.3150

Interoperability Need: Representing Patient Medical Encounter Diagnosis							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	SNOMED CT®	Final	Production	●●●●○	Yes	Free	N/A
Standard	ICD-10-CM	Final	Production	●●●●○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Value Set(s) and Starter Set(s):**
• Use of SNOMED CT® codes should generally be chosen from three axes: Clinical finding, Situation with explicit context, and Event. • The use of these standards may be further constrained by other standards and implementation specifications found elsewhere in the ISA. • Systems should be able to process (or at minimum display) data coded using the older ICD-9-CM standard, as this legacy content still exists and may be used for analysis/decision support/quality measurement needs, where retroactive analysis is often required, but ICD-9 should not be collected for new entries. NLM has maps from ICD-9-CM diagnosis and procedure codes to SNOMED CT to facilitate code translation and integration with newly collected SNOMED CT data: ▪ ICD-9-CM Diagnostic Codes to SNOMED CT ▪ ICD-9-CM Procedure Codes to SNOMED CT • A mapping from SNOMED CT® to ICD-10-CM is available from the National Library of Medicine to support semi-automated generation of ICD-10-CM codes from clinical data encoded in SNOMED CT for reimbursement and statistical	• Problem urn:oid:2.16.840.1.113883.3.88.12.3221.7.4 (SNOMED CT® code system) • Recommended starter set: CORE Problem List Subset urn:oid: 2.16.840.1.113762.1.4.1018.240

purposes. • HIPAA mandates the use of ICD-10 for pharmacy claims using NCPDP standards, while SNOMED is optional for this use.	

Family Health History

Interoperability Need: Representing Patient Family Health History

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●●●○○	No	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	●●●○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Some details around family genomic health history may not be captured by SNOMED CT®. • For clinical genomics purposes, the Human Phenotype Ontology (HPO) developed by Robinson, et al. and uses information from the Online Mendelian Inheritance in Man to generate its terms. It is popular within the genomics community, and is used by some organizations to describe "phenotypic abnormalities". • See LOINC projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	For Diagnosis and Conditions: • Problem Type 2.16.840.1.113883.3.88.12.3221.7.2 (LOINC® code system) • Problem urn:oid:2.16.840.1.113883.3.88.12.3221.7.4 (SNOMED CT® code system) For genomic data: • Gene Identifier: HGNC Value Set (2.16.840.1.113883.4.642.2.468) • Transcript Reference Sequence Identifier: NCBI vocabulary • DNA Sequence Variation Identifier: NCBI vocabulary • DNA Sequence Variation: HGVS nomenclature (2.16.840.1.113883.4.642.2.392) For family relationships and roles: • Personal Relationship Role Type urn:oid:2.16.840.1.113883.1.11.19563 • Personal And Legal Relationship Role Type urn:oid:2.16.840.1.113883.11.20.12.1

Functional Status/Disability

Interoperability Need: Representing Patient Functional Status and/or Disability							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard for observations	LOINC®	Final	Production	●●○○○	No	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	●○○○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Value Set(s) and Starter Set(s):**
• Resources for this interoperability need include: ▪ Social Security Association's Disability Determination Process ▪ American College of Occupational and Environmental Medicine additional resources on Functional Status/Disability. ▪ American Medical Association's "Guides to the Evaluation of Permanent Impairment, Sixth Edition" • The CMS Data Element Library also provides the ability to download assessment data elements, including functional status, and associated health IT standards from the: ▪ Inpatient Rehabilitation Facility Patient Assessment Instrument (IRF-PAI) ▪ Long-Term Care Hospital Continuity Assessment Record & Evaluation (CARE) Data Set (LCDS) ▪ Resident Assessment Instrument (RAI) Minimum Data Set (MDS) ▪ Outcome and Assessment Information Set (OASIS) • The interoperability need is directed to cover people's functional activities at the level of the individual, including activity limitations, the ability to participate in or be involved in all areas of life, and any participation restrictions as a person or member of society. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• MDS 3.0 v1.16.1 and IRF-PAI 2.0 and 3.0 - Functional abilities and goals - admission [CMS Assessment] (LOINC panel 88482-5) • MDS 3.0 v1.16.1 and IRF-PAI 2.0 and 3.0 - Functional abilities and goals - discharge [CMS Assessment] (LOINC panel 88483-3) • LCDS v4.00 - Functional abilities and goals [CMS Assessment] (LOINC panel 88238-1) • LCDS v4.00 - Functional abilities and goals -- planned discharge [CMS Assessment] (LOINC panel 88237-3) • OASIS D - Functional abilities and goals – Start of Care (SOC)/ Resumption of Care (ROC) [CMS Assessment] (LOINC panel 89572-2) • OASIS D - Functional abilities and goals - follow-up [CMS Assessment] (LOINC panel 88484-1) • OASIS D - Functional abilities and goals - discharge [CMS Assessment] (LOINC panel 89391-7)

Health Care Providers, Family Members and Other Caregivers

Interoperability Need: Representing Health Care Providers

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	National Plan and Provider Enumeration System National Provider Identifier (NPI)	Final	Production	●●●●○	Yes	Free	N/A
Standard	National Uniform Claim Committee (NUCC) Health Care Provider Taxonomy	Final	Production	●●●○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• NPPES permits non-billable care team members to apply for an NPI number to capture the concept of 'person'. • NPI taxonomy does not describe all roles associated with an individual's care team, however, NUCC Health Care Provider Taxonomy codes cover concepts of other health care providers.	• NUCC Healthcare Provider Taxonomy (HIPAA) value set OID:2.16.840.1.114222.4.11.1066

Interoperability Need: Representing Provider Role in Team Care Settings

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	SNOMED CT®	Final	Production	●●●○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• NUCCPT codes capture roles of direct care providers as well as other members of the care team as well as those provider supporting health services.	• NUCCPT Healthcare Provider Taxonomy : 2.16.840.1.114222.4.11.1066 • Pharmacy e-Health Information Technology Collaborative Occupations of Providers SNOMED CT value set 2.16.840.1.113762.1.4.1096.129

Interoperability Need: Representing Relationship Between Patient and Another Person

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 V3 Vocabulary	Final	Production	●●○○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• This value set is derived from the HL7 Vocabulary code system "RoleCode".	• Personal And Legal Relationship Role Type (VSAC OID

	2.16.840.1.1138883.11.20.12.1) • This value set can be used to record relationships based on personal or family ties or through legal assignment of responsibility.

Imaging (Diagnostics, Interventions and Procedures)

Interoperability Need: Representing Imaging Diagnostics, Interventions and Procedures

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●●●○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Radiological Society of North America (Radlex) and Regenstrief Institute (LOINC®) have harmonized terms for radiology procedures.	• Radlex LOINC Imaging Document Codes

Immunizations

Interoperability Need: Representing Immunizations – Administered

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 Standard Code Set CVX—Clinical Vaccines Administered	Final	Production	●●●●●	Yes	Free	N/A
Standard	HL7 Standard Code Set MVX -Manufacturing Vaccine Formulation	Final	Production	●●●●○	No	Free	N/A
Standard	National Drug Code	Final	Production	●●●●●	Yes	Free	N/A
Standard	RxNorm	Final	Production	Feedback requested	No	Free	N/A
Standard	Current Procedural Terminology (CPT)	Final	Production	●●●●○	No	$	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• HL7 CVX codes are designed to represent administered and historical immunizations and will not contain manufacturer-specific information. • If an MVX code is paired with a CVX (vaccine administered) code, the specific	• CVX: Vaccines Administered 2.16.840.1.113762.1.4.1010.6 • MVX: entire code set

trade named vaccine may be indicated providing further specificity as to the vaccines administered. • There is a potential issue with use of the National Drug Code regarding which code to use when there are multiple active ingredients in a single package or multiple separate ingredients that need to be mixed together. CDC has published guidance on NDC Unit of Use and Unit of Sale; it can be found at: https://www.cdc.gov/vaccines/programs/iis/2d-vaccine-barcodes/downloads/guidance-documenting-ndc.pdf • CPT and RxNorm are acceptable alternative code sets for local use, but are not the code sets federally required for exchange with immunization registries and thus may have limitations for interoperability across systems.	

Interoperability Need: Representing Immunizations – Historical

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 Standard Code Set CVX—Clinical Vaccines Administered	Final	Production	●●●●●	Yes	Free	N/A
Standard	HL7 Standard Code Set MVX -Manufacturing Vaccine Formulation	Final	Production	●●●●○	No	Free	N/A
Standard	RxNorm Vaccine Clinical Drug 2.16.840.1.113762.1.4.1010.8	Final	Production	Feedback Requested	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• CVX codes are designed to represent administered and historical immunizations and will not contain manufacturer-specific information. • When an MVX code is paired with a CVX (vaccine administered) code, the specific trade named vaccine may be indicated providing further specificity as to the vaccines administered. • MVX is rarely used to record historical vaccines; however, if a provider has the information available in that standard it should be captured and messaged as part of the historical vaccination record. • RxNorm is an acceptable alternative code set for local use, but it is not federally required for exchange with immunization registries and thus may have limitations for interoperability across systems.	• CVX: Vaccines Administered 2.16.840.1.113762.1.4.1010.6 • MVX: entire code set 2.16.840.1.114222.4.11.826 • RxNorm Vaccine Clinical Drug 2.16.840.1.113762.1.4.1010.8

Industry and Occupation

Interoperability Need: Representing Patient Industry and Occupation

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	CDC_Census 2010 Industry and Occupation System	In Development	Pilot	Feedback requested	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The CDC_Census 2010 system is used by the National Institute for Occupational Safety and Health (NIOSH) to classify industry and occupation entries in over 1 million records each year from health data collection systems such as health surveys, registries, and death records. They are based on the US Census' industry and occupation classification system, which is based on the North American Industry Classification System (NAICS) and Standard Occupational Classification (SOC) System. The CDC_Census system provides useful detail for the care provider and meets other federal requirements for statistical analysis. • NIOSH is developing updates to these value sets to include more detailed titles based on the Census Bureau Alphabetical Indexes for Industry and Occupation and will incorporate military service and occupation. A tool for collecting patient industry and occupation titles in electronic health records is also under development.	• Representing Industry ▪ LOINC code for Past or Present Industry: 86188-0 'History of Occupation Industry' ▪ LOINC code for Usual Industry: 21844-6 'Usual Industry' ▪ LOINC Answer List LL3925-6 contains the PHIN VADS value set: ▪ PHVS_Industry_CDC_Census2010 urn:oid:2.16.840.1.114222.4.11.7187 • Representing Occupation ▪ LOINC Code for Past or Present Occupation: 11341-5 'History of Occupation' ▪ LOINC code for Usual Occupation: 21843-8 'Usual Occupation' ▪ LOINC Answer List LL3926-4 contains the PHIN VADS value set: ▪ PHVS_Occupation_CDC_Census2010 urn:oid:2.16.840.1.114222.4.11.7186

Laboratory

Interoperability Need: Representing Laboratory Tests

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●●●○○	Yes	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	●○○○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Laboratory test and observation work in conjunction with values or results which can be answered numerically or categorically. If the value/result/answer to a laboratory test and observation is categorical that answer should be represented with the SNOMED CT® terminology. • A single lab test with a single result will have the same LOINC® term for its order	• LOINC Top 2000+ Lab Observations - US Version OID: 1.3.6.1.4.1.12009.10.2.3

and result answer, but a panel order will have an order LOINC® term and multiple result LOINC® terms for each result in the panel. • A single lab test with a single result may have the same LOINC® code for the order and the result or may have a more specific code in the result (for example if the order code was method less or did not declare the system property). A panel order will have an order LOINC® code and multiple result LOINC® terms for each result in the panel. • Guidance is available for using SNOMED CT® and LOINC® together. • See LOINC projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	

Medications

Interoperability Need: Representing Patient Medications

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	RxNorm	Final	Production	●●●●●	Yes	Free	N/A
Standard	National Drug Code (NDC)	Final	Production	●●●●○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• RxNorm is often used for the exchange of information; however, it may not be available for export and import by end users. • The use of NDC in conjunction with RxNorm can help minimize gaps in representing medications, including compounded products, over -the-counter medications, and herbals. • Immunizations are not considered medications for this interoperability need.	• Grouping Value Set: Medication Clinical Drug 2.16.840.1.113762.1.4.1010.4 ▪ Medication Clinical General Drug (2.16.840.1.113883.3.88.12.80.17) ▪ Medication Clinical Brand-specific Drug (2.16.840.1.113762.1.4.1010.5) (RxNorm). • Grouping Value Set: Clinical Substance 2.16.840.1.113762.1.4.1010.2 ▪ Medication Clinical Drug (2.16.840.1.113762.1.4.1010.4) (RxNorm) ▪ Unique Ingredient Identifier - Complete Set (2.16.840.1.113883.3.88.12.80.20) (UNII)

Nursing

Interoperability Need: Representing Clinical/Nursing Assessments

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●●○○○	No	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	●●○○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Concepts for observation values from SNOMED CT® should generally be chosen from two axes: Clinical finding and Situation with explicit context. • When representing validated scales, LOINC® should be used for the question and LOINC® answers (LA Codes) should be used for the answers. • Question/Answer (name/value) pairs are a valuable representation of assessments, but best practices indicate the full question with answer should be included in communication. • See LOINC projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• Inpatient Rehabilitation Facility Patient Assessment Instrument (IRF-PAI) - Version 2.0 [CMS Assessment]: LOINC® 88329-8 • Long-Term Care Hospital Continuity Assessment Record & Evaluation (CARE) Data Set (LCDS) v.4.0 [CMS Assessment]: LOINC® 87509-6 • Resident Assessment Instrument (RAI) Minimum Data Set (MDS) v.1.16 Nursing Home Comprehensive (NC) item set [CMS Assessment]: LOINC® 88954-3 • Outcome and Assessment Information Set (OASIS) - Version D - Start of Care [CMS Assessment]: LOINC® 88373-6

Interoperability Need: Representing Nursing Interventions

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	SNOMED CT®	Final	Production	Feedback requested	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• According to the Journal of Nursing Education nursing interventions can be defined as "any task that a nurse does to or for the patient" or "something that directly leads to a patient outcome." • Coded interventions may be linked as related/dependent concepts to observations and assessments, as appropriate. • The Procedure axis of SNOMED CT is the terminology used for Nursing Interventions.	• A resource available is a map set from ICNP to SNOMED CT.

Interoperability Need: Representing Outcomes for Nursing

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	Feedback requested	No	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	Feedback requested	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Other ANA-recognized terminologies should be mapped to LOINC® for comparison across health systems and/or transmission. • Use LOINC® if the outcome is a measurement. • Use SNOMED CT® if the outcome is an observed assessment that a patient state has improved. In addition, when the outcome is recorded as an assertion (e.g., normotensive, afebrile, etc.) the terminology to be used is SNOMED CT®. • See LOINC projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• Feedback requested.

Interoperability Need: Representing Patient Problems for Nursing

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observation values	SNOMED CT®	Final	Production	Feedback requested	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The use of SNOMED CT® for this interoperability need, codes should generally be chosen from two axes: Clinical finding and Situation with explicit context. • Local and other ANA-recognized terminologies should be converted to SNOMED CT® for comparison across health systems and/or transmission.	• Starter Set: Nursing Problem List Subset of SNOMED CT

Patient Clinical "Problems" (i.e., conditions)

Interoperability Need: Representing Patient Clinical "Problems" (i.e., Conditions)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observation values	SNOMED CT®	Final	Production	●●●●●	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The use of SNOMED CT® for this interoperability need, codes should generally be chosen from three axes: Clinical finding, Situation with explicit context, and Event. • SNOMED CT® supports the combination of codes (post-coordination) to generate new meaning. Codes from other axes can be used in post-coordination. The need to pick multiple codes may be seen as a disadvantage. This can be avoided if post-coordination is limited to the backend, exposing a single code for users to pick. • For more information about observations and observation values, see Appendix I for an informational resource developed by the Health IT Standards Committee.	• PHINVADS Problem Value Set 2.16.840.1.113883.3.88.12.3221.7.4 • CORE Problem List Subset urn:oid: 2.16.840.1.113762.1.4.1018.240

Preferred Language

Interoperability Need: Representing Patient Preferred Language (Presently)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Request for Comment (RFC) 5646	Final	Production	Feedback requested	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• RFC 5646 encompasses ISO 639-1, ISO 639-2, ISO 639-3 and other standards related to identifying preferred language.	• Language urn:oid:2.16.840.1.113883.1.11.11526 (based off RFC 4646. This will be updated to reflect RFC 5646).

Pregnancy Status

Interoperability Need: Representing Patient Pregnancy Status

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●○○○○	No	Free	No
Standard for observation values	SNOMED CT®	Final	Production	●○○○○	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• When patient is currently pregnant, additional data fields should be collected, including: date of pregnancy status, estimated delivery date or gestational age. See applicable value sets and Recommendations from Collaboration of the Health IT Policy and Health IT Standards Committees' Public Health Task Force (Excel File Download, 31KB) for more details. • There are ongoing deliberations within CDC and other organizations to identify the best location to capture pregnancy status in provider workflows. • See LOINC® projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• LOINC® code: 82810-3 Pregnancy status • SNOMED CT®: ▪ Patient currently pregnant (finding), 77386006 ▪ Not pregnant (finding), 60001007 ▪ Possible pregnancy (finding), 102874004 • LOINC® codes: 11778-8 Estimated Delivery Date or 21299-3 Gestational age method

Procedures

Interoperability Need: Representing Dental Procedures Performed

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Code on Dental Procedures and Nomenclature (CDT)	Final	Production	●●●●○	Yes	$	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Feedback requested.	• Feedback requested.

Interoperability Need: Representing Medical Procedures Performed

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	SNOMED CT®	Final	Production	●●●●●	Yes	Free	N/A
Standard	CPT-4	Final	Production	●●●●●	Yes	$	N/A
Standard	HCPCS®	Final	Production	●●●●●	Yes	Free	N/A
Standard	ICD-10-PCS	Final	Production	●●●●○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• ICD-10-PCS is primarily a billing code used only in inpatient settings. • CPT and HCPCS are codes used to report procedures and services in outpatient procedures. • ICD-10-PCS is named in the 2015 Edition certification rules as an optional code set for procedures. • SNOMED CT procedure codes can be used to describe treatment in any clinical setting and is not tied to billing, but can be cross-mapped to corresponding ICD-10-PCS and CPT/HCPCS codes.	• Feedback requested.

Race and Ethnicity

Interoperability Need: Representing Patient Race and Ethnicity

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	OMB standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, Oct 30, 1997	Final	Production	●●●●○	Yes	Free	N/A
Standard	CDC Race and Ethnicity Code Set Version 1.0	Final	Production	Feedback requested	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The CDC Race and Ethnicity Code Set Version 1.0, which expands upon and can be rolled up to the OMB standards may help to further define race and ethnicity for this interoperability need as it allows for multiple races and ethnicities to be chosen for the same patient. • The high-level race/ethnicity categories in the OMB Standard may be suitable for statistical or epidemiologic or public health reporting purposes but may not be adequate in the pursuit of precision medicine and enhancing therapy or clinical decisions. • LOINC® provides observation codes for use in the observation / observation value pattern for communicating race and ethnicity. • The LOINC® answers for Race look similar to CDC/HL70005, but don't match; this may be confusing to implementers. • When clinically significant, the patient's "race" or "ethnicity" should be managed using an "Ask on Order Entry" question (AOE). This process is defined in the eDOS Implementation Guide developed through the ONC Standards & Interoperability Framework, and is designed work in conjunction with the LOI Implementation Guide, also developed through the ONC S&I Framework. For example, Glomerular Filtration Rate, Estimated (eGFR) results reference ranges vary based on race.	• Race (5 codes): Race Category Excluding Nulls urn:oid:2.16.840.1.113883.3.2074.1.1.3 • Race (extended set, 900+codes): Race urn:oid:2.16.840.1.113883.1.11.14914 • Ethnicity: Ethnicity urn:oid:2.16.840.1.114222.4.11.837 • Ethnicity (extended set, 43 codes): Detailed Ethnicity urn:oid:2.16.840.1.114222.4.11.877

Research

Interoperability Need: Representing Data for Biomedical and Health Services Research Purposes							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	Clinical Data Interchange Standards Consortium (CDISC) Controlled Terminology Standards for Data Collection through Clinical Data Acquisition Standards Harmonization (CDASH), Hosted by NCI-EVS	Final	Production	●●●○○	Yes	Free	N/A
Standard	Clinical Data Interchange Standards Consortium (CDISC) Controlled Terminology Standards for Data Aggregation through Study Data Tabulation Model (SDTM) (including QRS, Medical Device and Pharmacogenomics Data), Hosted by NCI-EVS	Final	Production	●●●●●	Yes	Free	N/A
Standard	Clinical Data Interchange Standards Consortium (CDISC) Controlled Terminology for Therapeutic Area Standards Hosted by NCI-EVS	Final	Production	●○○○○	Yes	Free	N/A
Standard	Clinical Data Interchange Standards Consortium (CDISC) Controlled Terminology for Data Collection for Protocol Hosted by NCI-EVS	Final	Production	Feedback requested	No	Free	N/A
Standard	Clinical Data Interchange Standards Consortium (CDISC) Controlled Terminology for Analysis Dataset Model (ADaM) Hosted by NCI-EVS	Final	Production	●●●○○	Yes	Free	N/A
Standard	Observational Medical Outcomes Partnership (OMOP) Common Data Model (CDM)	Final	Production	●●●●○	No	Free	Yes
Standard	Sentinel Common Data Model	Final	Production	●●○○○	No	Free	N/A
Standard	National Cancer Institute (NCI) Enterprise Vocabulary Service (EVS)	Final	Production	●●●○○	No	Free	N/A
Standard	National Cancer Institute (NCI) cancer Data Standards Repository (caDSR)	Final	Production	●●●○○	No	Free	N/A

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	National Cancer Institute (NCI) Metathesaurus	Final	Production	●●●○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The adoption and federally required levels for using CDISC SDTM for QRS, Medical Devices and Pharmacogenomics purposes vary.	• Feedback requested.

Sex at Birth, Sexual Orientation and Gender Identity

Interoperability Need: Representing Patient Gender Identity

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●●●○○	No	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	●●●○○	Yes	Free	N/A
Standard for observation values	HL7 Version 3 Null Flavor	Final	Production	●●●○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Collect discrete structured data on patient gender identity, sex, and sexual orientation following recommendations issued in a report by The Fenway Institute and the Institute of Medicine. • Even though clinicians and their patients would benefit from having these data in patient records, this does not suggest that it is the sole responsibility of clinicians and their staffs to collect these sensitive data. • When patients provide a response to this question in a patient portal, it could contradict with the information collected by providers. • See LOINC projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• Gender identity. LOINC® code: 76691-5 • Male. SNOMED CT® code: 446151000124109 • Female. SNOMED CT® code: 446141000124107 • Female-to-Male (FTM)/Transgender Male/Trans Man. SNOMED CT® code: 407377005 • Male-to-Female (MTF)/Transgender Female/Trans Woman. SNOMED CT® code: 407376001 • Genderqueer, neither exclusively male nor female. SNOMED CT® code: 446131000124102 • Additional gender category or other, please specify. HL7 Version 3 code: OTH • Choose not to disclose. HL7 Version 3 code: ASKU

Interoperability Need: Representing Patient Sex (At Birth)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●●●●●	No	Free	N/A
Standard for observation values	For Male and Female, HL7 Version 3 Value Set; for Administrative Gender Unknown, HL7 Version 3 Null Flavor	Final	Production	●●●●●	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s)
• HL7 Version 2 and 3 need to be harmonized. • See LOINC projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• LOINC® code: 76689-9 Sex assigned at birth • Administrative Gender (HL7 V3) 2.16.840.1.113883.1.11.1 • ONC's 2015 Edition certification requirements reference the following value set for birth sex that use a combination of HL7 Version 3 (V3) Standard value set for Administrative Gender and NullFlavor: (1) M ("Male") (2) F ("Female") (3) UNK ("Unknown") (HL7 V3 NullFlavor code)

Interoperability Need: Representing Patient-Identified Sexual Orientation

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●●○○○	No	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	●●○○○	Yes	Free	N/A
Standard for observation values	HL7 Version 3 Null Flavor	Final	Production	●●●○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Collect discrete structured data on patient gender identity, sex, and sexual orientation following recommendations issued in a report by The Fenway Institute and the Institute of Medicine of the National Academies. • See LOINC® projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• LOINC® code: 76690-7 Sexual orientation • ONC's 2015 Edition certification requirements reference the following value set for sexual orientation. Codes from (i) through (iii) are SNOMED CT® and (iv) through (vi) are from HL7 Version 3: (i) *Lesbian, gay or homosexual.* 38628009 (ii) *Straight or heterosexual.* 20430005 (iii) *Bisexual.* 42035005 (iv) *Something else, please describe.* nullFlavor OTH (v) *Don't know.* nullFlavor UNK (vi) *Choose not to disclose.* nullFlavor ASKU • SNOMED CT® code: Sexually attracted to neither male nor female sex 765288000 (Not required in ONC's 2015 Edition certification requirements)

Social, Psychological, and Behavioral Data

Interoperability Need: Representing Alcohol Use

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●○○○○	Yes	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	Feedback requested	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The Alcohol Use Disorder Identification Test - Consumption [AUDIT-C] consists of the first 3 questions of the World Health Organization's 10-question AUDIT alcohol screening that can help identify patients who are hazardous drinkers or have active alcohol use disorders (including alcohol abuse or dependence), is best suited for this interoperability need. • See LOINC projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• AUDIT-C panel (LOINC® code 72109-2) ▪ AUDIT-C member codes: ▪ LOINC® code 68518-0 (with LOINC® answer list ID LL2179-1) ▪ LOINC® code 68519-8 (with LOINC® answer list ID LL2180-9) ▪ LOINC® code 68520-6 (with LOINC® answer list ID LL2181-7) ▪ AUDIT-C total score (LOINC® code 75626-2) • AUDIT panel (LOINC code 72110-0) • AUDIT panel total score (LOINC code 75624-7)

Interoperability Need: Representing Depression

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●○○○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The Patient Health Questionnaire 2 item (PHQ-2) is a 2-question initial screen for symptoms of depression in the past 2 weeks. It consists of the first 2 questions of the PHQ-9, which can determine if an individual meet criteria for a depressive disorder, and is best suited for this interoperability need. • See LOINC projects in the Interoperability Proving Ground.	• PHQ-2 panel LOINC® code 55757-9 ▪ PHQ-2 member codes ▪ PHQ-2 Q1 LOINC® 44250-9 ▪ PHQ-2 Q2 LOINC® 44255-8 ▪ PHQ-2 Total Score LOINC® 55758-7 • PHQ-9 panel LOINC® code 44249-1

Interoperability Need: Representing Exposure to Violence (Intimate Partner Violence)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●○○○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The HARK (Humiliation, Afraid, Rape, Kick) is a four-question screen for identifying women who have experienced intimate partner violence (IPV) in the past year and may help women disclose IPV in general practice. It is best suited for use with this interoperability need. • See LOINC projects in the Interoperability Proving Ground.	• HARK panel LOINC® code 76499-3 ▪ HARK member codes: ▪ LOINC® code 76500-8 (with LOINC® answer list ID LL963-0) ▪ LOINC® code 76501-6 (with LOINC® answer list ID LL963-0) ▪ LOINC® code 76502-4 (with LOINC® answer list ID LL963-0) ▪ LOINC® code 76503-2 (with LOINC® answer list ID LL963-0) ▪ HARK total score LOINC® code 76504-0

Interoperability Need: Representing Financial Resource Strain

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●○○○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• A single-item question used to determine the patient's overall financial resource strain developed from the Coronary Artery Risk Development in Young Adults (CARDIA) study is best suited for this interoperability need. • See LOINC® projects in the Interoperability Proving Ground.	• Overall financial resource strain (CARDIA) LOINC® code 76513-1 • LOINC® answer list ID LL3266-5

Interoperability Need: Representing Level of Education

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●○○○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• A single question, "current educational attainment" used to determine the highest grade or level of school completed or highest degree received, developed as part of	• Current educational attainment (NHANES) LOINC® code 63504-5 • LOINC® answer list ID LL1069-5

the National Health and Nutrition Examination Survey (NHANES) is best suited for this interoperability need. • See LOINC® projects in the Interoperability Proving Ground.	

Interoperability Need: Representing Physical Activity

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●○○○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The Two-question screen, "moderate to strenuous activity in last 7 days" adapted by SAMHSA from the Kaiser Permanente Exercise Vital Sign screen of physical activity is best suited for this interoperability need. • See LOINC projects in the Interoperability Proving Ground.	• How many days of moderate to strenuous exercise, like a brisk walk, did you do in the last 7 days? LOINC® code 68515-6 • On those days that you engaged in moderate to strenuous exercise, how many minutes, on average, did you exercise? LOINC® code 68516-4 • Responses use applicable UCUM unit of measure.

Interoperability Need: Representing Social Connection and Isolation

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●○○○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• The Social connection and isolation panel is a set of five questions used to assess the number of types of social relationships on which a patient is connected and not isolated. It was developed for the National Health and Nutrition Examination Survey (NHANES), and is best suited for this interoperability need. • See LOINC projects in the Interoperability Proving Ground.	• Social connection and isolation panel LOINC® code 76506-5 ▪ Member codes: ▪ LOINC® code 63503-7 (with LOINC answer list ID LL1068-7) ▪ LOINC® code 76508-1 ▪ LOINC® code 76509-9 ▪ LOINC® code 76510-7 ▪ LOINC® code 76511-5 (with LOINC answer list ID LL963-0) ▪ Social isolation score LOINC® code 76512-3

Interoperability Need: Representing Stress

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●○○○○	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• A single-question stress measure primarily tested in Scandinavian populations is part of the Occupational Stress Questionnaire™ (Q41) developed by the Finnish Institute of Occupational Health is best suited for this interoperability need. • See LOINC projects in the Interoperability Proving Ground.	• Occupational Stress Questionnaire™ Q41 LOINC® code 76542-0 • LOINC® answer list LL3267-3

Tobacco Use (Smoking Status)

Interoperability Need: Representing Patient Tobacco Use (Smoking Status)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard for observations	LOINC®	Final	Production	●●●●●	No	Free	N/A
Standard for observation values	SNOMED CT®	Final	Production	●●●●●	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• There are limitations in SNOMED CT® for this interoperability need, which include, but not limited to: not being able to capture severity of dependency, level of use, quit attempts, lifetime exposure, and use of e-Cigarettes. • LOINC® includes codes that support recording smoking status in the CDC's preferred (and sometimes required) responses (e.g., Tobacco smoking status NHIS[76691-5]) and other kinds of observations (e.g., Have you smoked at least 100 cigarettes in your entire life [PhenX] [63581-3] or How old were you when you first started smoking cigarettes every day [PhenX] [63609-2]. • See LOINC® projects in the Interoperability Proving Ground. • For more information about observations and observation values, see Appendix III for an informational resource developed by the Health IT Standards Committee.	• 'Tobacco smoking status NHIS' LOINC 72166- 2 • Current Smoking Status urn:oid:2.16.840.1.113883.11.20.9.38 • ONC's 2015 Edition certification requirements reference the following value set for smoking status. Codes from SNOMED CT® : ▪ Current every day smoker. 449868002 ▪ Current some day smoker. 428041000124106 ▪ Former smoker. 8517006 ▪ Never smoker. 266919005 ▪ Smoker, current status unknown. 77176002 ▪ Unknown if ever smoked. 266927001 ▪ Heavy tobacco smoker. 428071000124103 ▪ Light tobacco smoker. 428061000124105 • Additional tobacco-related codes: ▪ Date quit tobacco smoking: LOINC 74010-0 ▪ Date quit smokeless tobacco: LOINC 88030-2 ▪ User of smokeless tobacco (finding): SNOMED CT® 713914004 ▪ Smokeless tobacco non-user (finding): SNOMED CT® 451381000124107 ▪ Former smokeless tobacco user (finding): SNOMED-CT® 456711000124105 ▪ Chews tobacco (finding): SNOMED-CT® 81703003 ▪ Snuff user (finding): SNOMED-CT® 228494002 ▪ User of moist powdered tobacco (finding): SNOMED-CT® 228504007 ▪ Electronic cigarette user (finding): SNOMED-CT® 722499006 ▪ Passive smoker (finding): SNOMED-CT® 43381005 ▪ Exposure to second hand tobacco smoke (event): SNOMED-CT® 16090371000119103 ▪ No known exposure to tobacco smoke (finding): SNOMED-CT® 711563001

Units of Measure

Interoperability Need: Representing Units of Measure (For Use with Numerical References and Values)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	The Unified Code for Units of Measure	Final	Production	●●●○○	Yes	Free	Yes Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• UCUM is a syntax for representing units of measure for use with numerical references and values. It is not an enumerated set of codes. • The case sensitive version is the correct unit string to be used for interoperability purposes. • Per public comments received, there may be some limitations with UCUM in the laboratory domain that remain unresolved. • The abbreviations used for a few of the units of measure listed in the UCUM standard are currently on lists of prohibited abbreviations from the Institute for Safe Medication Practice (ISMP). • Some abbreviations for units of measure include symbols which may be in conflict with other HL7 standards. • Some abbreviations for units are nonstandard for human understanding.(For example, if a result for a White Blood Cell count is 9.6 x 103/µL, the UCUM recommendation for rendering this value in a legacy character application is 9.6 x 10*3/uL. Because the "*" is a symbol for multiplication in some systems.) This recommendation may result in errors either by the information system or the human reading the result. • Some other abbreviations used in UCUM are not industry standard for the tests that use these units of measure.	• Units Of Measure Case Sensitive 2.16.840.1.113883.1.11.12839 (most frequently used codes) • "Table of Example UCUM Codes for Electronic Messaging" published by the Regenstrief Institute, Inc. Value set is made available at http://loinc.org/usage/units and identified by the OID 1.3.6.1.4.1.12009.10.3.1

Vital Signs

Interoperability Need: Representing Patient Vital Signs

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	LOINC®	Final	Production	●●●●●	Yes	Free	N/A
Standard	ISO/IEEE 11073 Health informatics - Medical / health device communication standards	Final	Pilot	●●●○○	No	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• See Section I – Units of Measure for discussion of units of measure used with quantitative observations. • See LOINC® projects in the Interoperability Proving Ground. • See LOINC collaboration with IEEE for information on the Medical Device Code Mapping Table, which provides linkages between LOINC terms and IEEE EMB/11073 standard.	• Vital Sign Result urn:oid:2.16.840.1.113883.3.88.12.80.62

Section II: Content/Structure Standards and Implementation Specifications

Admission, Discharge, and Transfer

Interoperability Need: Sending a Notification of a Long Term Care Patient's Admission, Discharge and/or Transfer Status to the Servicing Pharmacy

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 10.6	Final	Production	●●●●●	Yes	$	No
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The "Census Message" transaction allows for long-term and post-acute care settings to notify the servicing pharmacy of a patient's admission, discharge and/or transfer status. • See NCPDP projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Sending a Notification of a Patient's Admission, Discharge and/or Transfer Status to Other Providers							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	HL7 2.5.1 (or later) ADT message	Final	Production	●●●●●	No	Free	No
Implementation Specification	IHE Patient Administration Management (PAM) Integration Profile	Final	Feedback requested	Feedback requested	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**
• A variety of transport protocols are available for use for ADT message delivery. Trading partners will need to determine which transport tools best meet their interoperability needs, however, Direct (referenced further in Section III: Push Exchange), has been noted as a prominent option for transport, particularly where HIE networks are not in place or not being used for this purpose. • See HL7 V2 projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** – Identifies the purpose for the transaction.

Care Plan

Interoperability Need: Documenting and Sharing Care Plans for a Single Clinical Context							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Release 2.1	Balloted Draft	Pilot	●●●○○	Yes	Free	Yes
Emerging Standard	*HL7 Fast Healthcare Interoperability Resources (FHIR), STU 3*	*In Development*	*Pilot*	●○○○○	*No*	*Free*	*No*
Emerging Implementation Specification	*HL7 Resource Care Plan (v1.0.2)*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**
• The care plan as expressed in the C-CDA standard does not attempt to represent the longitudinal care plan; rather it represents a "snapshot" of a care plan at a single point in time for transmission to other providers and teams to ensure continuity of care. • The Care Plan Domain Analysis Model is used as a reference model for C-CDA care plan documents in the context of the longitudinal care plan. • FHIR Resources are in various stages of maturity. Please refer to the FHIR website for updates on specific profiles and their progress. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • See CDA and FHIR projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Documenting and Sharing Medication-Related Care Plans by Pharmacists

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	NCPDP Pharmacist eCare Plan Version 1.0 Guidance on the Use of the HL7 CDA Consolidated Templates for Clinical Notes R2.1 Care Plan	Final	Production	●●○○○	No	$	Yes[$]
Implementation Specification	HL7 CDA® R2 Implementation Guide: Pharmacist Care Plan Document, Release 1 - US Realm, Volume 1	Final	Production	●○○○○	No	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The two implementation specifications listed for this interoperability need are a result of a joint effort between HL7 and NCPDP to create a standardized, interoperable document for exchange of consensus-driven prioritized medication-related activities, plans and goals for an individual needing care Pharmacists work in multiple environments. This project was partially funded by ONC's High Impact Pilots Cooperative Agreement Program. The Community Pharmacy Enhanced Services Network maintains a listing of vendor participants from this program. • More than 100 value sets are currently captured in VSAC in support of this interoperability need. Search for "PharmacyHIT" to view them. • See this project in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Domain or Disease-Specific Care Plan Standards

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 CDA® R2 Implementation Guide: Personal Advance Care Plan Document, Release 1 - US Realm	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	HL7 CDA® R2 Implementation Guide: Clinical Oncology Treatment Plan and Summary, Release 1 – US Realm	Balloted Draft	Feedback requested	●●●○○	No	Free	No
Implementation Specification	IHE Quality, Research, and Public Health Technical Framework Supplement, Early Hearing Detection and Intervention (EHDI), Rev 2.1 Trial Implementation	Balloted Draft	Pilot	●●●○○	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The two HL7 CDA R2 IGs are based on C-CDA R2.1 and align with the Care Plan document specifications. The IHE Profile is based on HL7 V2.6 IG: Early	• Feedback requested.

Hearing Detection and Intervention (EHDI) Messaging, Release 1. • The Personal Advance Care Plan Document is for the domain of patient-authored goals, priorities and preferences, including but not limited to Advance Directives. • See CDA and IHE projects in the Interoperability Proving Ground.	

Interoperability Need: Sharing Patient Care Plans for Multiple Clinical Contexts

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Emerging Implementation Specification	*IHE Dynamic Care Planning (DCP), Rev 1.2 Trial Implementation*	*Balloted Draft*	*Pilot*	*Feedback requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See IHE projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Sharing Patient Care Teams for Care Planning in Multiple Clinical Contexts

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Emerging Implementation Specification	*IHE Dynamic Care Planning (DCP), Rev 1.1 Trial Implementation*	*Balloted Draft*	*Pilot*	*Feedback requested*	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Feedback requested.	• Feedback requested

Clinical Decision Support

Interoperability Need: Communicate Appropriate Use Criteria with the Order and Charge to the Filling Provider and Billing System for Inclusion on Claims

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Emerging Implementation Specification	*IHE: Clinical Decision Support Order Appropriateness Tracking (CDS-OAT)*	*Balloted Draft*	*Pilot*	*Feedback requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See IHE projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Provide Access to Appropriate Use Criteria

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Emerging Implementation Specification	*CDS Hooks Services*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes*
Emerging Implementation Specification	*HL7 FHIR Clinical Reasoning Module, FHIR STU Release 3*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The CDS Hooks specification describes the RESTful APIs and interactions between EHRs and CDS Services. • Note that the FHIR Implementation Guide: Clinical Quality Framework (CQF on FHIR) in STU 3 was incorporated into FHIR as a core implementation guide, FHIR Clinical Reasoning. • Note that the maturity level of FHIR resources may vary. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • See FHIR projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Shareable Clinical Decision Support

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 Cross-Paradigm Specification: Clinical Quality Language, Release 1, STU Release 2	Balloted Draft	Production	●●●○○	No	Free	Yes
Standard	HL7 Cross-Paradigm Specification: Clinical Quality Language, Release 1, STU Release 3	Balloted Draft	Production	●●●○○	No	Free	Yes
Standard	HL7 FHIR Profile: Quality (QI Core), STU Release 3	Balloted Draft	Pilot	●●○○○	No	Free	Yes
Standard	HL7 Version 3 Standard: Decision Support Service, Release 2	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	HL7 Implementation Guide: Clinical Decision Support Knowledge Artifact Implementation Guide, Release 1.3, Draft Standard for Trial Use.	Balloted Draft	Pilot	●●○○○	No	Free	No
Implementation Specification	HL7 FHIR Implementation Guide: Clinical Reasoning Module, FHIR STU Release 3	Balloted Draft	Pilot	●●○○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Note that the maturity level of FHIR resources may vary. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • See FHIR projects in the Interoperability Proving Ground.	• Feedback requested.

Clinical Quality Measurement and Reporting

Interoperability Need: Reporting Aggregate Quality Data to Quality Reporting Initiatives

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 Clinical Document Architecture (CDA®), Release 2.0, Final Edition	Final	Production	●●●●●	No	Free	No
Implementation Specification	HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture - Category III (QRDA III), DSTU Release 1	Final	Production	●●●●○	Yes	Free	Yes
Implementation Specification	HL7 Implementation Guide for CDA® Release 2: Quality Reporting Document Architecture - Category III (QRDA III), DSTU Release 2.1	Final	Production	●●●●○	Yes	Free	Yes
Implementation Specification	HL7 Fast Healthcare Interoperability Resources (FHIR) Clinical Reasoning STU 3	Final	Production	●●●●○	No	Free	Yes
Emerging Implementation Specification	*HL7 Fast Healthcare Interoperability Resources (FHIR) Clinical Reasoning STU 4*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• See CDA and QRDA projects in the Interoperability Proving Ground.
• Implementation Maturity:
  ○ STU Release 1: Used for 2017-2018 reporting
  ○ STU Release 2.1: Being used for reporting 2018, 2019 data.
	• Feedback requested

Interoperability Need: Reporting Patient-level Quality Data to Quality Reporting Initiatives

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture - Category I (QRDA I) DSTU Release 3.1 (US Realm)	Balloted Draft	Production	●●●●○	Yes	Free	Yes
Emerging Implementation Specification	*HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture - Category I (QRDA I) STU Release 4 (US Realm)*	*In Development*	*Pilot*	●○○○○	*Yes*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See CDA and QRDA projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Sharing Quality Measure Artifacts for Quality Reporting Initiatives

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 V3: Representation of the Health Quality Measures Format (eMeasure), DSTU Release 2.1	Balloted Draft	Pilot	●●●●○	No	Free	Yes
Implementation Specification	HL7 V3 Implementation Guide: Quality Data Model (QDM)-based Health Quality Measure Format (HQMF), Release 1.4 DSTU 4 (based on HQMF 2.1 – US Realm	Balloted Draft	Production	●●●●○	Yes	Free	Yes
Standard	HL7 Cross-Paradigm Specification: Clinical Quality Language (CQL), Release 1, STU Release 1.1	Balloted Draft	Production	●●○○○	No	Free	Yes
Implementation Specification	HL7 Version 3 Implementation Guide: Clinical Quality Language (CQL)-based Health Quality Measure Format (HQMF), Release 1.1 DSTU 2 (based on HQMF 2.1 - US Realm	Balloted Draft	Production	●●○○○	No	Free	Yes
Emerging Implementation Specification	*HL7 Version 3 Implementation Guide: Clinical Quality Language (CQL)-based Health Quality Measure Format (HQMF), Release 2 DSTU32 (based on HQMF 2.1 - US Realm*	*In Development*	*Pilot*	●●○○○	*No*	*Free*	*Yes*
Standard	HL7 FHIR Profile: Quality (QI Core), DSTU Release 1	Balloted Draft	Pilot	●○○○○	No	Free	Yes
Emerging Implementation Specification	*HL7 Fast Healthcare Interoperability Resources (FHIR) Clinical Reasoning STU Release 3*	*In Development*	*Pilot*	●○○○○	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Note that the maturity level of FHIR resources may vary. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • See FHIR projects in the Interoperability Proving Ground.	• Feedback requested.

Data Provenance

Interoperability Need:	Establishing the Authenticity, Reliability, and Trustworthiness of Content Between Trading Partners						
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	HL7 CDA® Release 2 Implementation Guide Data Provenance, Release 1 - US Realm	Balloted Draft	Pilot	●○○○○	No	Free	Yes - Open
Emerging Implementation Specification	*HL7® FHIR® Provenance Resource*	*Balloted Draft*	*Pilot*	*Feedback requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The first implementation specification listed is focused on data provenance representation for CDA R2 implementations and the use of CDA templates. • Note that the maturity level of FHIR resources may vary. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • The FHIR implementation specification listed 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 available within the resource. • See CDA & FHIR projects in the Interoperability Proving Ground.	• Feedback requested.

Diet and Nutrition

Interoperability Need: Exchanging Diet and Nutrition Orders Across the Continuum of Care

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 Version 3 Standard: Diet and Nutrition, STU Release 1	Balloted Draft	Pilot	●○○○○	No	Free	Yes
Emerging Implementation Specification	*HL7 FHIR Nutrition Order Resource*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes* *Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• FHIR Resources are in various stages of maturity. Please refer to the FHIR website for updates on specific profiles and their progress. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • In addition to the specifications listed above, work is underway to create a HL7 CDA R2 Implementation Guide: C-CDA R2.1 Supplemental Templates for Nutrition, Release 1 (US Realm). • See FHIR projects in the Interoperability Proving Ground.	• **System Authentication** - The information and process necessary to authenticate the systems involved • **User Details** - identifies the end user who is accessing the data • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Drug Formulary & Benefits

Interoperability Need: The Ability for Pharmacy Benefit Payers to Communicate Formulary and Benefit Information to Prescribers Systems

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	NCPDP Formulary and Benefits v3.0	Final	Production	●●●●●	Yes	$	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• NCPDP Formulary and Benefits v3.0 does not provide real-time patient-level benefit information. • NCPDP is developing a Real Time Prescription Benefit standard that should be monitored as a potential emerging implementation specification.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Electronic Prescribing

Interoperability Need: Allows a Pharmacy to Notify a Prescriber of Prescription Fill Status

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 10.6	Final	Production	●●○○○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- The following transactions need to be implemented for interoperability purposes:
  - SCRIPT 10.6 & SCRIPT 2017071 -
    - RxFill: sent from a pharmacy to a prescriber or long term or post-acute care (LTPAC) facility indicating the FillStatus (dispensed, partially dispensed, not dispensed or returned to stock, transferred to another pharmacy) of the new, refill or resupply prescriptions for a patent
  - SCRIPT 2017071 -
    - RxFillIndicator: Informs the pharmacy of the prescriber's intent for fill status notifications for a specific patient/medication
    - RxFillIndicatorChange: Sent by the prescriber to the pharmacy to indicate that the prescriber is changing the types of RxFill transactions that were previously requested, where the prescriber may modify the fill status of transactions previously selected or cancel future RxFill transactions
    - When transferring a prescription, the RxFillRequestIndicator should be passed to the new pharmacy as part of the prescription information. If it supports the RxFill transaction, the pharmacy to which the prescription was transferred is responsible to send the appropriate Physician RxFill Request Flag with each subsequent dispensing event.
- The prescriber must electronically send the prescription via the NCPDP SCRIPT standard in order for the prescriber's system to receive RxFill transactions, and ensures the correct matching between the original prescription and the subsequent RxFill transactions.
- Adoption of RxFill may be improved by allowing prescribers to specify which prescriptions are to receive RxFill transactions and which RxFill message types to receive. Additionally, prescribers may choose to receive RxFill transactions for patients receiving certain medications. EMRs may also provide additional capabilities to support RxFill message handling and prescriber preferred notifications that may provide process improvements such as limiting the number

Applicable Security Patterns for Consideration:

- **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication.
- **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.
- **Authentication Enforcer** – centralized authentication processes.
- **Authorization Enforcer** – specifies access control policies.
- **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).
- **Assertion Builder** – define processing logic for identity, authorization and attribute statements.
- **User Role** – identifies the role asserted by the individual initiating the transaction.
- **Purpose of Use** - Identifies the purpose for the transaction.

of transactions received, the cost of transactions, privacy concerns and information overload. • Both the pharmacy and the prescriber must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive verify, status, or error transactions. • See NCPDP projects in the Interoperability Proving Ground.	

Interoperability Need: Allows the Pharmacy to Respond to Prescriber with a Change on a New Prescription

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 10.6	Final	Production	●●●○○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• The following transactions need to be implemented for interoperability purposes:
  ○ SCRIPT 10.6 -
  ▪ RxChg, originated from the pharmacy to request a change in the original prescription.
  ▪ Chgres, originated from the prescriber in response to the RxChg message.
  ○ SCRIPT 2017071 -
  ▪ RxChangeRequest, originated from the pharmacy to request:
  • a change in the original prescription (new or fillable)
  • validation of prescriber credentials
  • a prescriber to review the drug requested
  • obtaining a prior authorization from the payer for the prescription
  ▪ FollowUpRequest, originated from the pharmacy to:
  • notify prescribers that this is a follow-up RxRenewalRequest or RxChangeRequest transaction, when the prescriber has not responded to the first RxRenewalRequest or first RxChangeRequest transaction in a reasonable amount of time.
  • Not sent on the original request of the RxRenewalRequest or RxChangeRequest transaction
  ▪ RxChangeResponse, originated from the prescriber to respond:
  • to a prescription change request from a pharmacy
  • to a request for a prior authorization from a pharmacy
	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication.
	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.
	• **Authentication Enforcer** – centralized authentication processes.
	• **Authorization Enforcer** – specifies access control policies.
	• **Credential Tokenizer** – encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).
	• **Assertion Builder** – define processing logic for identity, authorization and attribute statements.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** - Identifies the purpose for the transaction

• to a prescriber credential validation request from a pharmacy ▪ Options allowed when generating an RxChangeResponse in response to an RxChangeRequest from a pharmacy: • Approved: Grant the RxChangeRequest when the prescriber concurs with the request. The prescriber must submit an RxChangeResponse equal to what the pharmacy requested. • ApprovedWithChanges: When the information submitted in the RxChangeRequest does not include all elements constituting a fillable prescription; the prescriber should include all information. • Denied: Denies the RxChangeRequest with information that explains the denial. • Validated: Sent by the prescriber system in response to an RxChangeRequest for prescriber authorization. • The receiving pharmacy should handle Approved, ApprovedWithChanges, and Validated responses as a fillable NewRx where the original linked prescription/order is discontinued. A Denied response should be directed to a review queue where the Denial reason code is displayed. • Both the pharmacy and the prescriber must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive verify, status, or error transactions. • See NCPDP projects in the Interoperability Proving Ground.	

Interoperability Need: Allows a Pharmacy to Request a New Prescription For a New Course of Therapy or to Continue Therapy

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Emerging Standard	*HL7 FHIR Medication Request*	*In Development*	*Pilot*	*Feedback Requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The following transactions need to be implemented for interoperability purposes: ○ SCRIPT 2017071 - ▪ NewRxRequest: This transaction is a request from a pharmacy to a prescriber for a new prescription for a patient • NewRxResponseDenied: This transaction is a denied response to a previously sent NewRxRequest (If	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer** – encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).

approved, a NewRx would be sent) ○ A NewRxResponseDenied response may occur when the NewRxRequest cannot be processed or if information is unavailable • Both the prescriber and the pharmacy must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive verify, status, or error transactions. • See NCPDP projects in the Interoperability Proving Ground.	• **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction

Interoperability Need: Allows a Pharmacy to Request Additional Refills

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 10.6	Final	Production	●●●●○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The following transactions need to be implemented for interoperability purposes: ○ SCRIPT 10.6 – ▪ Refreq, originated from the pharmacy to the prescriber requesting additional refills. ▪ Refres, originated from the prescriber to the pharmacy with a Rx authorization for refills; the response to a Refreq message. ○ SCRIPT 2017071 - ▪ RxRenewalRequest, originated from the pharmacy to request additional refills beyond those originally prescribed • FollowUpRequest, originated from the pharmacy to: ○ notify prescribers that this is a follow-up RxRenewalRequest or RxChangeRequest transaction, when the prescriber has not responded to the first RxRenewalRequest or first RxChangeRequest transaction in a reasonable amount of time. ○ not sent on the original request of the RxRenewalRequest or RxChangeRequest transaction ▪ RxRenewalResponse, originated from the prescriber to respond to the request • Options allowed when generating an	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer** – encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction

RxRenewalResponse to an RxRenewalRequest from a pharmacy:

- Approved: Grant the RxRenewalRequest as requested by the pharmacy, or, when the pharmacy does not request a specific number of fills (PharmacyRequestedRefills is not present) and the prescriber approves any number of fills
- ApprovedWithChanges: Grant the RxRenewalRequest, approving a NumberOfRefills different than the number requested by the pharmacy or when the information submitted in the RxRenewalRequest does not include all elements constituting a fillable prescription; the prescriber should include all information
- Denied: Deny the RxRenewalRequest as requested by the pharmacy
  - In a Denied response, the only new meaning that should be conveyed to the pharmacy is information that explains the denial. It is recommended that the prescribing software update the NumberOfRefills to zero and leave all other data as is in the RxRenewalResponse
- Replace: Data is allowed to be changed except the patient DateOfBirth. If patient DateOfBirth changes, a Denied response would be sent, and then a NewRx would follow

- The receiving pharmacy might handle each of these responses differently. Approved, ApprovedWithChanges, and Replace responses might be directed to a fulfillment queue, where a Denied response might be directed to a review queue
- The Replace response should be used if there are any changes beyond what is outlined in the Response Element

- RxRenewalRequest should never be responded to with a NewRx, as this would result in duplicate valid prescriptions
- DeniedNewPrescriptionToFollow response is not to be sent in an RxRenewalResponse for this version of SCRIPT. However, the DeniedNewPrescriptionToFollow response could be received in an RxRenewalResponse from a previous version of SCRIPT and is included for backwards compatibility. DeniedNewPrescriptionToFollow response only exists for entities

that need to map this version to a previous version of SCRIPT that does not support a Replace. • Both the pharmacy and the prescriber must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive verify, status, or error transactions. • See NCPDP projects in the Interoperability Proving Ground.	

Interoperability Need: Allows a Pharmacy to Request, Respond to, or Confirm a Prescription Transfer

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2013101	Final	Production	●●●○○	No	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• The following transactions need to be implemented for interoperability purposes:
  ○ RxTransferRequest: Used when the pharmacy is asking for a transfer of one or more prescriptions for a specific patient to the requesting pharmacy
  ▪ The transfer is for a fillable prescription which may be:
  • yet to be filled
  • on hold
  • open (active) fills
  • current therapy (defined as drug therapy that, based upon the most recent fill date, quantity and instructions, should still be active)
  • allowed to be transferred by law/regulation
  ▪ If multiple specific prescriptions are to be transferred, but not all prescriptions, a separate RxTransferRequest must be sent for each specific prescription
  ○ RxTransferResponse: The response from the transferring pharmacy to the requesting pharmacy to the RxTransferRequest which includes the prescription(s) being transferred or a rejection of the transfer request
  ○ RxTransferConfirm: Used by the pharmacy receiving (originally requesting) the transfer to confirm that the transfer prescription has been received and the transfer is complete
  ○ The RxFill Transaction <FillStatus><Transferred> is originated by the transferring pharmacy once the <RxTransferConfirm> is received from the transfer to pharmacy. This transaction is used to notify the prescriber when a prescription has been transferred to another pharmacy and can no longer
	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.
	• **Authentication Enforcer** – centralized authentication processes.
	• **Authorization Enforcer** – specifies access control policies.
	• **Credential Tokenizer** – encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).
	• **Assertion Builder** – define processing logic for identity, authorization and attribute statements.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** - Identifies the purpose for the transaction

be filled at the original pharmacy. The RxTransfer transaction will identify if the receiving pharmacy supports RxFill. • Both the pharmacy and the prescriber must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive verify, status, or error transactions. • See NCPDP projects in the Interoperability Proving Ground.	

Interoperability Need: Allows a Prescriber or a Pharmacy to Request a Patient's Medication History

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 10.6	Final	Production	●●○○○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• The following transactions need to be implemented for interoperability purposes:
  ○ RxHistoryRequest: a request from a prescriber or a pharmacy for a list of medications that have been prescribed, dispensed, claimed or indicated (OTCs) by a patient
  ▪ This patient-specific transaction supplies enough information to uniquely identify the patient
  ○ RxHistoryResponse: a response to an RxHistoryRequest containing a patient's medication history; includes the medications that were dispensed or obtained within a certain timeframe, optionally including the prescriber that prescribed it
  ▪ The receiver must evaluate the Consent for accurate reporting
  ▪ Returns with loops of Medication, HistorySource, Prescriber, Pharmacy, and Patient elements when appropriate
  ▪ HistorySource and FillNumber elements are included, when appropriate, so prescribers are able to de-duplicate records from multiple sources that reflect the same medication dispensing, and to help determine patient compliance with a prescription
  • Helps the prescriber determine if follow-up contact is required regarding the medication records
• RxHistoryRequest and RxHistoryResponse may be sent directly or through an intermediary.
• Medication history transactions may be exchanged among prescribers, pharmacies, or payers, and may include adjudicated claims and/or pharmacy dispensed/point of sale prescription information.
• It is recommended that prescribers request Medication History from all applicable
	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication.
	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.
	• **Authentication Enforcer** – centralized authentication processes.
	• **Authorization Enforcer** – specifies access control policies.
	• **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).
	• **Assertion Builder** – define processing logic for identity, authorization and attribute statements.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** - Identifies the purpose for the transaction.

sources, whenever appropriate, to ensure the most complete view of a patient's medication history. The Medication History may be reconciled with the prescriber's patient record for improved medication management and to assist in clinical decision support. • Both the sender and receiver must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive verify, status, or error transactions. This may also include hospitals and/or Accountable Care Organizations (ACOs). • See NCPDP projects in the Interoperability Proving Ground.	

Interoperability Need: Allows a Prescriber to Cancel a Prescription

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 10.6	Final	Production	●●○○○	Yes	$	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• The following transactions need to be implemented for interoperability purposes:
  ○ SCRIPT 10.6 -
  ▪ CanRx: a request from a prescriber to a pharmacy to not fill a previously sent prescription.
  ▪ CanRes: a response from a pharmacy to a prescriber to acknowledge a cancel request; the response to a CanRx.
  ○ SCRIPT 2017071 -
  ▪ CancelRx: a request from the prescriber to the pharmacy to not fill a previously sent prescription
  • must contain pertinent information for the pharmacy to be able to find the prescription in their system (patient, medication (name, strength, dosage form), prescriber, prescription number if available)
  • changes can be indicated in the MessageRequestCode in the CancelRx transaction
  ▪ CancelRxResponse: a response from the pharmacy to the prescriber to acknowledge a CancelRx
  • used to denote if the cancellation is Approved or Denied
  • DenialReasonCode should be sent when a CancelRx is denied
	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication.
	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.
	• **Authentication Enforcer** – centralized authentication processes.
	• **Authorization Enforcer** – specifies access control policies.
	• **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).
	• **Assertion Builder** – define processing logic for identity, authorization and attribute statements.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** - Identifies the purpose for the transaction.

▪ When a Long Term care (LTC) prescriber has the need to modify an order and notify the pharmacy, the prescriber system will always send a CancelRx and a NewRx, regardless of the type of change • Both the prescriber and the pharmacy must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive verify, status, or error transactions. • See NCPDP projects in the Interoperability Proving Ground.	

Interoperability Need: Allows a Prescriber to Prescribe Medication Using Weight-Based Dosing

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Structured and Codified Sig Format Implementation Guide Version 2.1	Final	Production	●○○○○	No	$	No
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Included in the Structured and Codified Sig Format of electronic prescribing transactions are elements, fields and values that are directly related to the prescriber's instructions for use. • The following elements of the Sig are required when Structured Sig is sent: o Code system o Dose o Route Of Administration • The following elements of the Sig are conditional (only required when prescriber specifies) when Structured Sig is sent: o Vehicle o Site of Administration o Timing o Duration o Maximum Dose Restriction o Indication • The following elements of the Sig are required when Structured Sig is sent *and when dose is to be calculated*: o Dose Calculation ▪ Used where a body metric such as metric weight (kg) or surface area (m*2) is used to calculate a dose for a patient. ▪ May often be used in conjunction with the Rate within TimingAndDuration and/or the Vehicle.	• LOINC 2.63 codes supporting SCRIPT 2017071 <Observation> segment: o 8302-2 Body height, measured [LOINC] o 3141-9 Body weight, measured [LOINC] o 3140-1 Body surface area, derived [LOINC]

• The SCRIPT 2017071 Observation element in the NewRx transaction supports the use of a patient's height, weight and other vital signs:
  ○ Inclusion of VitalSign (most recent patient's height and weight) and ObservationDate (YYYY-MM-DD height and weight observed/taken) is required for patients 18 years old and younger on all new and renewal prescriptions from a prescriber to a pharmacy.
  ▪ If the height and/or weight have changed and a prescriber is sending an approved renewal response, the response should be coded as Approved with Changes.
• ObservationDate is now mandatory when Observation Segment Measurement is sent.
• ObservationNotes may contain other pertinent information pertaining to weight-based calculations.	

Interoperability Need: Allows a Prescriber to Request, Cancel or Appeal Prior Authorization for Medications

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2013101	Final	Production	●●●○○	No	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• The prescriber system must receive timely Formulary & Benefit file updates from payers/intermediaries, giving group-level formulary and coverage information (including PA flags) for use when ordering medications.
• The following ASC X12 patient eligibility transactions enhance the PA Request transactions by supplying the prescriber system with the patient's pharmacy benefit information, and need to be implemented for interoperability purposes:
  ○ Eligibility Request (ASC X12 270)
  ○ Eligibility Response (ASC X12 271)
• The following SCRIPT 2017071 PA transactions need to be implemented for interoperability purposes:
  ○ PAInitiationRequest and PAInitiationResponse
  ○ PARequest and PAResponse
  ○ PAAppealRequest and PAAppealResponse
  ○ PACancelRequest and PACancelResponse
• Both the prescriber and the payer/processor/pharmacy benefits manager (PBM) must have their systems configured for these transactions in order to facilitate successful exchange, including the ability to send or receive status or error messages.
	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication.
	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.
	• **Authentication Enforcer** – centralized authentication processes.
	• **Authorization Enforcer** – specifies access control policies.
	• **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).
	• **Assertion Builder** – define processing logic for identity, authorization and attribute statements.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** - Identifies the purpose for the transaction

• See NCPDP projects in the Interoperability Proving Ground.	

Interoperability Need: Allows a Prescriber to Request a Patient's Medication History from a State Prescription Drug Monitoring Program (PDMP)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 10.6	Final	Production	●●○○○	No	$	No
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Emerging Standard	*HL7 FHIR Implementation Guide: US Meds STU2*	*Balloted Draft*	*Pilot*	*Feedback Requested*	*No*	*$*	*No*
Emerging Implementation Specification	*CDS Hooks Services*	*Balloted Draft*	*Pilot*	*Feedback Requested*	*No*	*Free*	*Yes*
Emerging Implementation Specification	*SMART on FHIR*	*Final*	*Feedback requested*	*Feedback Requested*	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• The following transactions need to be implemented for interoperability purposes:
  ○ RxHistoryRequest: a request from a prescriber for a list of medications that have been prescribed, dispensed, claimed or indicated (OTCs) by a patient to a state Prescription Drug Monitoring Program (PDMP).
  ▪ This patient-specific transaction supplies enough information to uniquely identify the patient
  ○ RxHistoryResponse: a response from a PDMP to an RxHistoryRequest containing a patient's medication history; includes the medications that were dispensed or obtained within a certain timeframe, optionally including the prescriber that prescribed it
  ▪ PDMP must evaluate the Consent for accurate reporting
  ▪ Returns with loops of Medication, HistorySource (pharmacy), Prescriber, Pharmacy, and Patient elements
  ▪ HistorySource and FillNumber elements are included, when appropriate, so prescribers are able to de-duplicate records from multiple sources that reflect the same medication dispensing, and to help determine patient compliance with a prescription
  • Helps the prescriber determine if follow-up contact is required regarding the medication records
	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication.
	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.
	• **Authentication Enforcer** – centralized authentication processes.
	• **Authorization Enforcer** – specifies access control policies.
	• **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).
	• **Assertion Builder** – define processing logic for identity, authorization and attribute statements.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** - Identifies the purpose for the transaction.

• RxHistoryRequest and RxHistoryResponse may be sent directly or through an intermediary • Both the prescriber and the Prescription Monitoring Drug Program (PDMP) must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive status, or error transactions. • The HL7 FHIR Implementation Guide: US Meds STU2 includes US Meds Prescription Drug Monitoring Program (PDMP) mapping. • SMART on FHIR defines a mechanism for interoperable "SMART Apps" that can be plugged in to EHRs and other Health IT systems. Each SMART App can expose a user interaction, and can access data in the underlying system. This presents a powerful way to extend EHR capabilities via "pluggable" app functionality. Dozens of SMART apps are available, including apps for medication management, pain management, and PDMP-EHR integration, with more expected in the future. These apps serve many different clinical needs, yet they all use the same underlying FHIR-based API functionality. • When using the SMART on FHIR model, the authentication model uses OAuth2. Except for "Secure Communication", the security patterns listed do not apply. • See NCPDP projects in the Interoperability Proving Ground.	

Interoperability Need: Representing Data for Biomedical and Health Services Research Purposes

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Pilot	●○○○○	No	$	Yes
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 10.6	Final	Production	●●●●●	Yes	$	Yes
Emerging Standard	*HL7 FHIR Medication Request*	*In Development*	*Pilot*	*Feedback requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• The following transactions need to be implemented for interoperability purposes:
  ○ SCRIPT 10.6 & SCRIPT 2017071 -
  ▪ NewRx: This transaction is a new prescription sent from the prescriber to the pharmacy electronically so that it can be dispensed to a patient
  ○ SCRIPT 2017071 -
  ▪ NewRxRequest: This transaction is a request from a pharmacy to a prescriber for a new prescription for a patient
  • NewRxResponseDenied: This transaction is a denied
	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.
	• **Authentication Enforcer** – centralized authentication processes.
	• **Authorization Enforcer** – specifies access control policies.
	• **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).
	• **Assertion Builder** – define processing logic for identity, authorization and attribute statements.

response to a previously sent NewRxRequest (If approved, a NewRx would be sent) o A NewRxResponseDenied response may occur when the NewRxRequest cannot be processed or if information is unavailable • Both the prescriber and the pharmacy must have their systems configured for the transaction in order to facilitate successful exchange, including the ability to send or receive verify, status, or error transactions. • See NCPDP projects in the Interoperability Proving Ground.	• **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Family Health History (Clinical Genomics)

Interoperability Need: Representing Family Health History for Clinical Genomics

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 Version 3 Standard: Clinical Genomics; Pedigree	Balloted Draft	Production	●○○○○	No	Free	No
Implementation Specification	HL7 Version 3 Implementation Guide: Family History/Pedigree Interoperability, Release 1	Balloted Draft	Production	●○○○○	No	Free	No
Emerging Implementation Specification	*HL7 Fast Healthcare Interoperability Resources (FHIR), STU 3*	*Final*	*Pilot*	*Feedback requested*	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s) for Consideration:
• There is no widely recognized vocabulary to capture family genomic health history, but several vocabularies/value sets are available for consideration. • Further constraint of this standard and implementation specification may be required to support this interoperability need. • The Office of the National Coordinator for Health Information Technology (ONC), in partnership with National Institutes of Health (NIH), created Sync for Genes to strengthen genomic data sharing, a key component of the Precision Medicine Initiative. This project is also in alignment with the recommendations made by the Precision Medicine Task Force under the Health IT Standards Committee (HITSC) to advance data standards, address relevant privacy policies, and advance innovations in health IT that support precision medicine. Sync for Genes is the first step toward integrating clinical genomics into the point-of-care by expediting the use of standards, such as Health Level 7 (HL7®) Fast Healthcare Interoperability Resource (FHIR®), to enable and improve patient's ability to seamlessly share their genomics information via point-of-care applications, such as application programming interfaces (APIs). Sync for Genes supports a critical element of sharing genomic data amplifying the ability to seamlessly share genomic information for	According to HIMSS, the following vocabularies/value sets may be considered: • Gene Identifier: HGNC Value Set • Transcript Reference Sequence Identifier: NCBI vocabulary • DNA Sequence Variation Identifier: NCBI vocabulary • DNA Sequence Variation: HGVS nomenclature

research and commercial purposes. Below are the HL7 FHIR Clinical Genomic profiles that were tested as part of the Sync for Genes work: ○ **Family Health History Genetics** ▪ https://www.hl7.org/fhir/pushpull.html ○ **Sequencing Quality and Regulatory Genomics** ▪ https://www.hl7.org/fhir/STU3/sequence.html ▪ https://www.hl7.org/fhir/STU3/bundle.html ▪ https://www.hl7.org/fhir/STU3/capabilitystatement.html • The HL7 FHIR® Resource: FamilyMemberHistory and associated FamilyMemberHistory-Genetic profile are most appropriate for this interoperability need. • The HL7 Version 2.5.1 Implementation Guide: Lab Results Interface (LRI) Version 1, STU 3 - US Realm includes a section that regards genomic information variants. It may be used as an option for meeting this interoperability need until FHIR® resources are more mature. • The U.S. Surgeon General also offers the My Family Health Portrait, allowing individuals to enter their family health history details to share with their family members and/or healthcare providers, learn about risk for conditions that can be hereditary, and be saved as a resource that can be maintained and updated over time. • See FHIR projects in the Interoperability Proving Ground.	

Healthy Weight

Interoperability Need: Sending Healthy Weight Information

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE Quality, Research and Public Health Technical Framework Supplement – Healthy Weight (HW)	Balloted Draft	Pilot	●○○○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Integrating the Healthcare Enterprise (IHE) Healthy Weight Profile Childhood obesity surveillance systems utilize either measured (e.g., NHANES) or parent/self-report height and weight to calculate BMI. The profile also includes the HL7 Occupational Data for Health (ODH) template. • Public health agencies have been studying the relationship between obesity and work factors; for example, the prevalence of obesity has been shown to vary substantially by occupation. • See IHE projects in the Interoperability Proving Ground.	• **System Authentication** - The information and process necessary to authenticate the systems involved. • **User Details** - identifies the end user who is accessing the data. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Images

Interoperability Need: Format of Medical Imaging Reports for Exchange and Distribution

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Digital Imaging and Communications in Medicine (DICOM)	Final	Production	●●●●●	No	Free	Yes
Implementation Specification	PS3.20 Digital Imaging and Communications in Medicine (DICOM) Standard – Part 20: Imaging Reports using HL7 Clinical Document Architecture.	Final	Production	●○○○○	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• DICOM defines both its own encoding of reports and templates for encoding narrative reports and machine-generated output as DICOM Structured Reports (SR) for use within imaging systems. • DICOM Part 20 is an implementation guide for HL7 CDA r2. • DICOM also defines a Diagnostic Imaging Report HL7 CDA Template, which is intended to supersede the C-CDA Diagnostic Imaging Report.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Format of Radiation Exposure Dose Reports for Exchange and Distribution

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	DICOM PS3.3 2017e A.35.8 X-Ray Radiation Dose SR IOD	Final	Production	●●○○○	No	Free	Yes - Open
Implementation Specification	DICOM PS3.3 2017e A.35.14 Radiopharmaceutical Radiation Dose SR IOD	Final	Production	●●○○○	No	Free	Yes - Open
Implementation Specification	DICOM PS3.3 2017e A.35.18.1 Patient Radiation Dose SR IOD	Final	Production	●●○○○	No	Free	Yes - Open

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• These reports record radiation dose in three forms: ▪ The dose related information provided by an exposing device, e.g., CT, as reported by the device.	• Feedback requested.

▪ The dose related information about a radiopharmaceutical administration, as reported by the administering system. ▪ The patient or organ absorbed dose based on exposure information, patient characteristics, and patient model. • See DICOM projects in the Interoperability Proving Ground.	

Interoperability Need: Format of Radiology Reports for Exchange and Distribution

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE Management of Radiology Report Templates (MRRT)	Balloted Draft	Pilot	Feedback requested	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See IHE projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Medical Image Formats for Data Exchange and Distribution

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Digital Imaging and Communications in Medicine (DICOM)	Final	Production	●●●●●	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Use Image Acquisition Technology Specific Service/Object Pairs (SOP) Classes.	• Feedback requested.

Laboratory

Interoperability Need: Identify Linkages Between Vendor IVD Test Results and Standard Codes

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	LIVD – Digital Format for Publication of LOINC to Vendor IVD Test Results	Final	Production	●○○○○	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The LIVD - Digital Format for Publication of LOINC to Vendor IVD Test results defines the digital publication of LOINC using vendor defined IVD tests associated with a set of predefined LOINC codes. LIVD assures that laboratory personnel select the appropriate LOINC codes for IVD test used by their laboratory. It also allows LIS systems to automatically map the correct IVD vendor test result to a LOINC code. LIVD was developed in collaboration with the members of the FDA IVD Semantic workgroup.	• Feedback requested.

Interoperability Need: Ordering Labs for a Patient

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 2.5.1	Final	Production	●●○○○	No	Free	No
Implementation Specification	HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Orders from EHR, Release 1 DSTU Release 2 - US Realm	*Balloted Draft*	Pilot	●○○○○	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• HL7 Laboratory US Realm Value Set Companion Guide, Release 1, September 2015, provides cross-implementation guide value set definitions and harmonized requirements. • Note that the implementation specification has been harmonized with the most current suite of Lab US Realm Implementation Guides and is scheduled for update in the HL7 January 2017 Ballot Cycle. • See HL7 V2 projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Receive Electronic Laboratory Test Results

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 2.5.1	Final	Production	●●○○○	No	Free	No
Implementation Specification	HL7 Version 2.5.1 Implementation Guide: S&I Framework Lab Results Interface, Release 1—US Realm [HL7 Version 2.5.1: ORU_R01] Draft Standard for Trial Use, July 2012	Balloted Draft	Production	●○○○○	Yes	Free	Yes
Emerging Implementation Specification	*HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Results Interface Implementation Guide, Release 1 DSTU Release 2 - US Realm*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• HL7 Laboratory US Realm Value Set Companion Guide, Release 1, September 2015, provides cross-implementation guide value set definitions and harmonized requirements. • The HL7 EHR-S Functional Requirements: S&I Framework Laboratory Results Messages, Release 1 - US Realm further clarifies sender/receiver responsibilities to achieve end-to-end interoperability for this interoperability need. • See HL7 V2 projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Support the Transmission of a Laboratory's Directory of Services to Health IT							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	HL7 2.5.1	Final	Production	●●○○○	No	Free	No
Implementation Specification	HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Test Compendium Framework, Release 2, DSTU Release 2 (also referred to as eDOS (Electronic Directory of Service)	Balloted Draft	Production	●○○○○	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• HL7 Laboratory US Realm Value Set Companion Guide, Release 1, September 2015, provides cross-implementation guide value set definitions and harmonized requirements. • Note that the current version has been harmonized with the most current suite of Lab US Realm Implementation Guides and is scheduled for update in the HL7 January 2017 Ballot Cycle. • See HL7 V2 projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Medical Device Communication to Other Information Systems/Technologies

Interoperability Need: Transmitting Patient Vital Signs from Medical Devices to Other Information Systems/Technologies							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	IHE-PCD (Patient Care Device Profiles)	Final	Production	●●●○○	No	Free	Yes
Implementation Specification	ITU H.810, H.811, H.812, H.812.5, and H.813	Final	Production	●●●○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• IHE-PCD, Continua and ITU refer to the IEEE 11073-10101 standard for nomenclature.	• Feedback requested.

• The following specific IHE-PCD profiles that best meet this interoperability need include: ▪ IHE-PCD (Patient Care Device Profiles) - Alert Communication Management (ACM) ▪ IHE-PCD (Patient Care Device Profiles) - Device Enterprise Communication (DEC) ▪ IHE-PCD (Patient Care Device Profiles) - Implantable Device – Cardiac Observation (IDCO) ▪ IHE-PCD (Patient Care Device Profiles) - Point-of-Care Infusion Verification (PIV) ▪ IHE-PCD (Patient Care Device Profiles) - Rosetta Terminology Mapping (RTM) • The Regenstrief LOINC/IEEE Medical Device Code Mapping Table allows enterprise information systems (i.e. ""Other information Systems/Technologies") to process vital signs and combine those observations with other types of information; it bridges the semantic map between IEEE 11073 10101 conformant medical devices and certified health IT or aligned information systems that use LOINC already for laboratory reports, document taxonomies, standard forms, questionnaires, assessments, social determinants, and screeners. • FDA cybersecurity recommendations for medical device manufacturers. • Design Considerations and FDA Pre-Market Submission Recommendations for Interoperable Medical Devices. • See IHE projects in the Interoperability Proving Ground.	

Patient Education Materials

Interoperability Need: Clinical Information Systems to Request Context-Specific Clinical Knowledge From Online Resources

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application ("Infobutton"), Knowledge Request, Release 2	Final	Production	●●●●○	Yes	Free	No
Implementation Specification	HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1	Final	Production	●●●○○	Yes	Free	No
Implementation Specification	HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4	Final	Production	●●●○○	Yes	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Feedback requested	• Feedback requested

Patient Identification Management

Interoperability Need: Patient Demographic Record Matching

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 2.5.1 (or later) ADT message	Final	Production	●●●●●	No	Free	Yes
Implementation Specification	IHE-PDQ (Patient Demographic Query)	Final	Production	●●●●●	No	Free	Yes
Implementation Specification	IHE-PIX (Patient Identifier Cross-Reference)	Final	Production	●●●●●	No	Free	Yes
Emerging Implementation Specification	*Implementation Guide for Expressing Context in Direct Messaging*	*Balloted Draft*	*Pilot*	*Feedback requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Chapter 3 of the HL7 Standard 2.5.1 named "Patient Administration" is the relevant chapter for Clinical and Administrative Domains. • NIST Special Publication 800-63, Revision 3 defines technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. These guidelines can be applied for identity proofing of any user or participant in healthcare such as clinicians, caregivers, patients and others. • The Implementation Guide for Expressing Context in Direct Messaging was designed to facilitate inter-organizational patient demographic record matching by standardizing the inclusion of patient demographic metadata in Direct messages. Direct is also listed in several Interoperability Needs in Section III: "Push Exchange". • Patient Identity Proofing is outside of the scope of this interoperability need but more information related to this topic is below: ▪ Identity Proofing. Each Signatory's security policy shall include the following elements to ensure appropriate identity proofing: ▪ (i) End Users (provider). Each Signatory shall identity proof participating End Users at Identity Assurance Level 2 (IAL2) prior to issuance of access credentials; and ▪ (ii) Individuals (patient). Each Signatory shall identity proof participating individuals at Identity Assurance Level 2 (IAL2) prior to issuance of access credentials; provided, however, that the Signatory may supplement identity information by allowing Participant staff to act as trusted referees and authoritative sources by using personal knowledge of the identity of	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

the individuals (e.g., physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges) collected during an antecedent in-person registration event. All collected personally identifiable information collected by the Signatory shall be limited to the minimum necessary to resolve a unique identity. • See HL7 V2, IHE, and Direct projects in the Interoperability Proving Ground.	

Patient Preference/Consent

Interoperability Need: Recording Patient Preferences for Electronic Consent to Access and/or Share their Health Information with Other Care Providers

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE Basic Patient Privacy Consents (BPPC)	Final	Production	●○○○○	No	Free	Yes – Open
Emerging Implementation Specification	*HL7 Implementation Guide for CDA®, Release 2: Consent Directives, Release 1*	*Final*	*Pilot*	●○○○○	*No*	*Free*	*N/A*
Emerging Implementation Specification	*IHE Advanced Patient Privacy and Consents (APPC)*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes*
Emerging Implementation Specification	*HL7 FHIR Consent Resource*	*In Development*	*Pilot*	●○○○○	*No*	*Free*	*Yes*
Emerging Implementation Specification	*HL7 Contract Resource*	*In Development*	*Pilot*	●○○○○	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The IHE and CDA-based specifications operate in conjunction with the IHE XDS, XCA, and XDR profiles. • IHE BPPC may not support management of patient privacy across governmental jurisdictions which may have different regulations regarding access to patient data by providers, patients, governmental entities, and other organizations. • Along with security tokens and consent documents, security labels that are the critical third part of the Attribute-Based-Access-Control and SLS should be mentioned as well. Security Labels are used in CDA, FHIR, as well as the IHE	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g.,

Document Sharing (e.g. XDS), as described on the FHIR security page at https://www.hl7.org/fhir/security-labels.html. • Carequality is working to develop a technical method for distributing and identifying consent forms to be used as part of their Patient Consent Framework. • See IHE and FHIR projects in the Interoperability Proving Ground.	– SAML, Kerberos). • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction. • **Patient Consent Information** - Identifies the patient consent information that may be required before data can be accessed.

Public Health Reporting

Interoperability Need: Case Reporting to Public Health Agencies

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 CDA® R2 Implementation Guide: Public Health Case Report, Release 2: the Electronic Initial Case Report (eICR), Release 1, STU Release 1.1	Balloted Draft	Pilot	●●○○○	No	Free	Yes
Implementation Specification	HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.0 - US Realm	Balloted Draft	Pilot	●●○○○	No	Free	Yes - Open
Implementation Specification	IHE IT Infrastructure Technical Framework, Volume 1 (ITI TF-1): Integration Profiles, Section 17: Retrieve Form for Data Capture (RFD)	Balloted Draft	Pilot	●○○○○	No	Free	Yes
Implementation Specification	IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation	Balloted Draft	Pilot	●○○○○	No	Free	No
Emerging Standard	*FHIR electronic Case Reporting (eCR) Implementation Guide (Balloted Draft)* *FHIR electronic Case Reporting (eCR) Implementation Guide (Continuous Integration Build)*	*In Development*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Electronic Initial Case Report (eICR) and the Reportability Response are paired together in pilot implementations to build a complete workflow. • Retrieve Form for Data Capture and Structured Data Capture are paired together in pilot implementation to build a complete workflow. • Electronic case reporting involves reporting to State and/or Local jurisdictions. It is not yet widespread. • Structured Data Capture Implementation Guide does not currently restrict vocabulary to standard vocabulary sets, and may require further implementation guidance for case reporting purposes.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).

• The IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation Guide does not support automated initiation of sending of case reports. It can support manual entry into an electronic form as follow-up to an initial case report submission.
• The FHIR electronic Case Reporting (eCR) Implementation Guide is included with both its balloted implementation guide and a link to the FHIR continuous build. The later, as a continuous integration build, may at any point in time be unavailable, incoherent, or undergoing rapid change.
• Some additional implementation guides related to public health reporting follow. Reporting is often captured under a specialized registry with associated standards when not specified as a separate measure. These include:
  ○ Early Hearing Detection and Intervention (EHDI)
  ○ Office of Populations Affairs (OPA) Family Planning Reporting IHE Profile
• Note that the maturity level of FHIR resources may vary. The FHIR Maturity Model and each of the levels is described on the HL7 wiki.
• See FHIR and IHE projects in the Interoperability Proving Ground.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** - Identifies the purpose for the transaction.
	• FHIR Security Labels support compliance with laws, policies, and consent directives governing HIPAA PHI and specially protected information (SPI).

Interoperability Need: Data Submission for Title X Family Planning Annual Reporting

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Emerging Implementation Specification	*IHE Quality, Research, and Public Health Technical Framework Supplement Family Planning Version 2 (FPv2) Rev. 1.1 – Trial Implementation*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The HHS Office of Population Affairs (OPA) is currently engaged in an overhaul of their Family Planning Annual Reporting system, to enable the reporting of encounter level data from all of their Title X sites in a standard format and via a standard methodology. OPA is currently piloting two interoperability standards through this project and is intending to begin collecting data according to this new system in 2019. • Visit the Office of Population Affairs (OPA) website for more information about the Family Planning Annual Report, and The Family Planning Annual Report and Health Information Technology (Health IT) Initiative (FPAR 2.0).	• Feedback requested.

Interoperability Need: Electronic Transmission of Reportable Lab Results to Public Health Agencies

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 Version 2.5.1: Implementation Guide: Electronic Laboratory Reporting to Public Health (US Realm), Release 1 with Errata and Clarifications and ELR 2.5.1 Clarification Document for EHR Technology Certification	Final	Production	●●●●○	Yes	Free	Yes
Implementation Specification	HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 2 (US Realm)	Balloted Draft	Production	●○○○○	No	Free	No
Implementation Specification	HL7 Version 2.5.1 Implementation Guide: Laboratory Results Interface, Release 1 STU Release 3 - US Realm	Balloted Draft	Production	●○○○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Stakeholders should refer to the health department in their state or local jurisdiction to determine onboarding procedures, obtain a jurisdictional implementation guide if applicable, and determine which transport methods are acceptable for submitting ELR as there may be jurisdictional variation or requirements. • See HL7 V2 projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Exchanging Immunization Data with Immunization Registries

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.4	Final	Production	●●●●●	Yes	Free	Yes
Implementation Specification	HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5	Final	Production	●●●○○	Yes	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Stakeholders should refer to the health department in their state or local jurisdiction to determine onboarding procedures, obtain a jurisdictional implementation guide if	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication.

applicable, and determine which transport methods are acceptable for submitting immunization registry data as there may be jurisdictional variation or requirements. • HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5 – Addendum is also available. • See HL7 V2 projects in the Interoperability Proving Ground.	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Reporting Antimicrobial Use and Resistance Information to Public Health Agencies

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 Implementation Guide for CDA® Release 2 – Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm.	Final	Production	●○○○○	Yes	Free	No
Emerging Implementation Specification	*HL7 Implementation Guide for CDA Release 2 – Level 3: NHSN Healthcare Associated Infection (HAI) Reports Release 2, DSTU Release 2.0*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• This is a national reporting system to CDC. Stakeholders should refer to implementation guide for additional details and contract information for enrolling in the program. • See CDA projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Reporting Birth and Fetal Death to Public Health Agencies

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE Quality, Research and Public Health Technical Framework Supplement 10 Birth and Fetal Death Reporting-Enhanced (BFDR-E)	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	HL7 Version 2.6 Implementation Guide: Birth and Fetal Death Reporting, Release 1 STU Release 2 (US Realm - Standard for Trial Use)	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	HL7 Version 3 CDA R2 Implementation Guide: Birth and Fetal Death Reporting, Release 1 (US Realm - Standard for Trial Use)	Balloted Draft	Pilot	●○○○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Use of the listed NIST test tool **requires** digital certificates. Contact laura.rappleye@altarum.org for digital certification information.	• Feedback requested.

Interoperability Need: Reporting Cancer Cases to Public Health Agencies

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	Implementation Guide for Ambulatory Healthcare Provider Reporting to Central Cancer Registries, August 2012	Balloted Draft	Production	●●○○○	Yes	Free	Yes
Implementation Specification	HL7 CDA ® Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1 – US Realm	Balloted Draft	Production	●○○○○	Yes	Free	Yes
Implementation Specification	North American Association of Central Cancer Registries, Inc. (NAACCR), Standards for Cancer Registries, Volume V, Pathology Laboratory Electronic Reporting, Version 4.0, published April 2011	Final	Production	●●●●○	Yes	Free	Yes Yes
Emerging Implementation Specification	*IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Stakeholders should refer to the health department in their state or local jurisdiction to determine onboarding procedures, obtain a jurisdictional implementation guide if applicable, and determine which transport methods are acceptable for submitting cancer reporting data as there may be jurisdictional variation or requirements. Some jurisdictions may not support cancer case reporting at this time.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes.

• Note that the NAACCR specification listed has not been vetted through a Voluntary Consensus Standards Body (VSCB), however it references the HL7 V 2.5.1 standard and LOINC, and has been sponsored by a number of organizations working in the cancer registry space. • See CDA, IHE, and FHIR projects in the Interoperability Proving Ground.	• **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Reporting Death Records to Public Health Agencies

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE Quality, Research and Public Health Technical Framework Supplement Vital Records Death Reporting (VRDR) R 3.2	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	HL7 Version 2.6 Implementation Guide: Vital Records Death Reporting, Release 1 (US Realm - Standard for Trial Use)	Balloted Draft	Pilot	●○○○○	No	Free	Yes
Implementation Specification	HL7 CDA R2 Implementation Guide: Vital Records Death Reporting, Release 1 STU 2 - (US Realm) (Standard for Trial Use)	Balloted Draft	Pilot	●○○○○	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Feedback requested.	• Feedback requested.

Interoperability Need: Reporting Newborn Screening Results to Public Health Agencies

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 CDA® R2 Implementation Guide: Ambulatory Healthcare Provider Reporting to Birth Defect Registries, Release 1 - US Realm	Balloted Draft	Pilot	●○○○○	No	Free	Yes
Implementation Specification	HL7 Version 2.6 Implementation Guide: Critical Congenital Heart Defects (CCHD) pulse oximetry screening results, Release 1	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	HL7 Version 2.6 Implementation Guide: Early Hearing, Detection and Intervention (EHDI) Results Release 1	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	HE Quality, Research, and Public Health Technical Framework Supplement Newborn Admission Notification Information (NANI) Rev. 2.1 – Trial Implementation	Balloted Draft	Pilot	●○○○○	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• Use of the listed NIST test tool **requires** digital certificates. Contact laura.rappleye@altarum.org for digital certification information. • There is current work to update the listed "ambulatory" implementation guides to include hospital reporting capabilities and Zika-related information. • The "Newborn Admission Notification Information (NANI)" is included here because its functionality directly supports other standards under this heading.	• Feedback requested.

Interoperability Need: Reporting Syndromic Surveillance to Public Health (Emergency Department, Inpatient, and Urgent Care Settings)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 2.5.1	Final	Production	●●●●●	Yes	Free	No
Implementation Specification	PHIN Messaging Guide for Syndromic Surveillance: Emergency Department and Urgent Care Data Release 1.1 and Conformance Clarification for EHR Certification of Electronic Syndromic Surveillance, Addendum to PHIN Messaging Guide for Syndromic Surveillance	Final	Production	●●●●○	Yes	Free	Yes
Implementation Specification	PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings, Release 2.0 and Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015; Erratum to the CDC PHIN 2.0 Messaging Guide, April	Final	Pilot	●●●○○	Yes	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Stakeholders should refer to the health department in their state or local jurisdiction to determine onboarding procedures, obtain a jurisdictional implementation guide if applicable, and determine which transport methods are acceptable for submitting syndromic surveillance data as there may be jurisdictional variation or requirements. • An Erratum to the CDC PHIN 2.0 Implementation Guide was issued in August, 2015. Implementers should refer to this guide for additional information and conformance guidance. • See HL7 V2 projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Sending Health Care Survey Information to Public Health Agencies							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	HL7 Clinical Document Architecture (CDA®), Release 2.0, Final Edition	Final	Production	●●●●●	No	Free	No
Implementation Specification	HL7 Implementation Guide for CDA® R2: National Health Care Surveys (NHCS), Release 1 - US Realm	Balloted Draft	Pilot	●●○○○	No	Free	Yes
Implementation Specification	HL7 CDA® R2 Implementation Guide: National Health Care Surveys (NHCS), R1 DSTU Release 1.1 - US Realm	Balloted Draft	Pilot	●○○○○	No	Free	Yes
Implementation Specification	HL7 CDA® R2 Implementation Guide: National Health Care Surveys (NHCS), R1 DSTU Release 1.2 - US Realm	Balloted Draft	Pilot	●○○○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**
• This is a national reporting system to CDC. Stakeholders should refer to the National Health Care Survey Program for information on participation. • See CDA projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Research

Interoperability Need: Data Collection for Submission to Registries and Reporting Authorities							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	CDISC Clinical Data Acquisition Standards Harmonization (CDASH)	Final	Production	●●●○○	No	Free	N/A

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE-RFD (Retrieve Form for Data Capture)	Final	Production	Feedback Requested	No	Free	N/A
Implementation Specification	HL7 Clinical Document Architecture (CDA®), Release 2.0, Final Edition	Final	Production	●●●●●	Yes	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See IHE projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Pre-population of Research Forms from Electronic Health Records

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	CDISC Clinical Data Acquisition Standards Harmonization (CDASH)	Final	Production	●●●○○	No	Free	N/A
Standard	CDISC Shared Health And Research Electronic Library (SHARE)	Final	Production	●●●○○	No	Free	N/A
Implementation Specification	IHE-RFD (Retrieve Form for Data Capture)	Final	Production	●●●●○	No	Free	N/A
Implementation Specification	IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	IHE-CRD (Clinical Research Document)	Balloted Draft	Production	●●○○○	No	Free	N/A
Implementation Specification	IHE-XUA (Cross-Enterprise User Assertion)	Final	Production	●●●○○	No	Free	N/A
Implementation Specification	IHE-ATNA (Audit Trail and Node Authentication)	Final	Production	●●○○○	No	Free	N/A
Implementation Specification	IHE-DEX (Data Element Exchange)	Balloted Draft	Pilot	●○○○○	No	Free	N/A

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 FHIR Implementation Guide: Structured Data Capture (SDC) Release 1	Balloted Draft	Pilot	●○○○○	No	Free	N/A
Emerging Standard	*HL7 FHIR Audit Event*	*Balloted Draft*	*Production*	●●●○○	*No*	*Free*	*N/A*
Emerging Standard	*HL7 FHIR Questionnaire/Questionnaire Response*	*Balloted Draft*	*Pilot*	*Feedback Requested*	*No*	*Free*	*N/A*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• FHIR Resources are in various stages of maturity. Please refer to the FHIR website for updates on specific profiles and their progress. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • See IHE projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Registering a Clinical Trial

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	CDISC Clinical Trial Registry (CTR-XML)	Final	Pilot	●○○○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The CDISC Clinical Trial Registry (CTR-XML) is used internationally, but in the US, the primary area for registering Clinical Trials is via ClinicalTrials.gov. • CTR-XML standard is based on CDISC ODM. It is an extension of the ODM standard.	• Feedback requested.

Interoperability Need: Submission of Clinical Research Data Contained in EHRs and Other Health IT Systems for General Purpose or Preserving Specific FDA Requirements							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	IHE- RFD (Retrieve Form for Data Capture)	Final	Production	●●●●○	No	Free	N/A
Standard	HL7 Clinical Document Architecture (CDA®), Release 2.0, Final Edition	Final	Production	●●○○○	No	Free	N/A
Standard	CDISC Clinical Data Acquisition Standards Harmonization (CDASH)	Final	Production	●●●○○	No	Free	N/A
Standard	CDISC Operational Data Model (ODM)	Final	Production	●●●●●	No	Free	N/A
Standard	CDISC Protocol Representation Model (PRM)	Final	Production	●○○○○	No	Free	Yes
Standard	CDISC Study/Trial Design Model (SDM)	Final	Production	●○○○○	No	Free	N/A
Implementation Specification	IHE-RPE (Retrieve Protocol for Execution)	Balloted Draft	Production	●●○○○	No	Free	N/A
Implementation Specification	IHE-CRPC (Clinical Research Process Content)	Balloted Draft	Production	●●○○○	No	Free	N/A
Standard	CDISC Study Data Tabulation Model (SDTM)	Final	Feedback requested	Feedback requested	No	Free	No
Implementation Specification	CDISC Study Data Tabulation Model Implementation Guide	Final	Feedback requested	Feedback requested	No	Free	No
Implementation Specification	CDISC Therapeutic Area User Guides	Final	Feedback requested	Feedback requested	No	Free	No
Emerging Standard	*CDISC Pharmacogenomics/genetics (PGx) Implementation Guide*	*Balloted Draft*	*Feedback requested*	*Feedback requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Stakeholders should review 21CFR11 for more details. • See IHE projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need:	Submission of Clinical Research Data to FDA to Support Product Marketing Applications						
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	CDISC Study Data Tabulation Model (SDTM)	Final	Production	●●●●●	Yes	Free	Yes
Standard	CDISC Analysis Dataset Model (ADaM)	Final	Production	●●●○○	Yes	Free	N/A
Standard	CDISC Operational Data Model (ODM)	Final	Production	Feedback Requested	No	Free	Yes
Standard	CDISC Dataset-XML (ODM-Based)	Final	Production	●○○○○	No	Free	N/A
Standard	CDISC Define-XML (ODM-Based)	Final	Production	●●●●●	Yes	Free	N/A
Standard	CDISC Standard for the Exchange of Non-clinical Data (SEND)	Final	Production	●●●○○	Yes	Free	N/A
Implementation Specification	Study Data Tabulation Model Implementation Guide for Medical Devices (SDTMIG-MD)	Final	Production	●○○○○	No	Free	N/A
Standard	Therapeutic Area Standards (to complement the aforementioned CDISC foundational standards that apply across all therapeutic areas)	Final	Production	●○○○○	Yes	Free	N/A
Standard	CDISC Questionnaires, Ratings and Scales (QRS)	Final	Feedback requested	Feedback requested	No	Free	No
Emerging Implementation Specification	*CDISC Pharmacogenomics/genetics (PGx) Implementation Guide*	*Balloted Draft*	*Feedback requested*	*Feedback requsted*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• FDA published the draft guidance promoting use of EHRs in clinical research, in collaboration with ONC. (http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-drugs-	• Feedback requested.

gen/documents/document/ucm501068.pdf) • FDA CDER published a FRN focusing on Source Data Capture From Electronic Health Records: Using Standardized Clinical Research Data. (https://www.federalregister.gov/documents/2015/06/26/2015-15644/source-data-capture-from-electronic-health-records-using-standardized-clinical-research-data) • FDA CDER and CBER encourage the submission of study data in conformance to the data standards listed in the FDA Data Standards Catalog (DSC). Standardized study data will be required in submissions for clinical and non-clinical studies that start on or after December 17, 2016 (December 17, 2017 for INDs). See Data Standards Catalog: (http://www.fda.gov/ForIndustry/DataStandards/StudyDataStandards/default.htm) and the Data Standards Strategy: (http://www.fda.gov/downloads/drugs/developmentapprovalprocess/formssubmissionrequirements/electronicsubmissions/ucm455270.pdf) • Although CDISC standards are a requirement for CDER and CBER and not for CDRH, all three Centers promote the use of Real World Data (RWD) in EHRs, registries, administrative claims and mobile health technology to generate Real World Evidence regarding the safety and effectiveness of medical products. In addition, FDA collaborates closely with other standards development organizations including but not limited to HL7, IHE, X12, and NCPDP. • FDA CDRH and CBER published the draft guidance: Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices. (see http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM513027.pdf) • Therapeutic Area Standards, that apply across a number of therapeutic areas, include a series of IGs at different level of maturity, from development to final.	

Interoperability Need: Submit Adverse Event Report from an Electronic Health Record to Drug Safety Regulators

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE-RFD (Retrieve Form for Data Capture)	Final	Production	●●●●○	No	Free	N/A
Implementation Specification	IHE-DSC (Drug Safety Content)	Balloted Draft	Pilot	●○○○○	No	Free	N/A
Implementation Specification	IHE-CPRC (Clinical Research Process Content)	Balloted Draft	Production	●●○○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See IHE projects in the Interoperability Proving Ground.	• Feedback requested.

Segmentation of Sensitive Information

Interoperability Need: Data Segmentation of Sensitive Information							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	Consolidated HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1	Final	Production	●○○○○	Yes	Free	Yes
Standard	HL7 Clinical Document Architecture (CDA®), Release 2.0, Final Edition	Final	Production	●●●●●	Yes	Free	No
Emerging Implementation Specification	*Consent2Share FHIR Consent Profile Design*	*Final*	*Pilot*	*Feedback Requested*	*No*	*Free*	*No*
Emerging Implementation Specification	*IHE IT Infrastructure Technical Framework Volume 4 - National Extensions – Section 3.1 Data Segmentation for Privacy (DS4P)*	*Final*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**

• 2015 Edition Health IT Certification Criterion for DS4P (§ 170.315(b)(7) and § 170.315(b)(8)), requires the use of the cda Privacy Segmented Document template for certification.
• HL7 v3 Implementation Guide for DS4P provides CDA templates to enable privacy and segmentation markings at the document, section and entry (data element) levels:
  ○ cda Privacy Markings Section- specifies how a document, section, or entry may be constrained to specify privacy and security markings.
  ○ cda Privacy Segmented Section-may apply to any section of a C-CDA document if that section metadata (sensitivity, confidentiality) is different than the document's overall
  ○ Privacy Metadata Templates-support the exchange of protected information by annotating specific entries with several observations, policies and constraints. Examples include:
  ▪ cda Privacy Annotation-a set of security observations that allow for specific privacy metadata for an entry that overrides that of a document or section
  ▪ cda Protected Problem-combines a mandatory provenance and privacy annotations with the default constraints applied to a ProblemObservation
  ▪ cda Security Observation-a class of abstract templates to indicate
	• Feedback requested.

a security classification, control, category, or integrity criterion • Subclasses include Obligation, Confidentiality, Refrain Policy, and Purpose of Use Security Observations • Consent2Share FHIR Consent Profile specifies how Substance Abuse and Mental Health Services Administration's (SAMHSA) Consent2Share application and associated access control solution uses FHIR resources to represent and persist patient consent for treatment, research, or disclosure (e.g. 42 CFR Part 2, Title 38) • For C-CDA transmission, document level DS4P is required in the C-CDA General Header. Therefore, adoption levels may be higher for document level tagging (vs. section level). • See CDA and DS4P in the Interoperability Proving Ground.	

Summary Care Record

Interoperability Need: Support a Transition of Care or Referral to Another Health Care Provider

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 Clinical Document Architecture (CDA®), Release 2.0, Final Edition	Final	Production	●●●●●	No	Free	Yes
Implementation Specification	HL7 Consolidated CDA® Release 1.1 (HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, DSTU Release 1.1 - US Realm)	Balloted Draft	Production	●●●●●	Yes	Free	Yes
Emerging Implementation Specification	*HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Release 2.1*	*Balloted Draft*	*Pilot*	*Feedback requested*	*Yes*	*Free*	*Yes*
Emerging Implementation Specification	*IHE Patient Care Coordination Technical Framework Supplement 360 Exchange Closed Loop Referral (360X) Rev. 1.1 – Trial Implementation*	*Balloted Draft*	*Pilot*	●○○○○	No	*Free*	No
Emerging Implementation Specification	*NCPDP Specialized Standard*	*Final*	*Feedback requested*	●○○○○	No	*$*	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• There are several specific document templates within the C-CDA implementation specification. Trading partners will need to ensure that their systems are capable of supporting specific document templates. • HL7 provides a C-CDA Example repository which contains a set of example C-CDA files that have undergone a review and vetting process to ensure completeness and rigor.	• Feedback requested.

• The IHE 360X specification listed is designed to track and manage referrals across health IT platforms. • The NCPDP Specialized Standard supports request/referral for Medication Therapy Management services. • Implementers should explore use of emerging CDA on FHIR and C-CDA on FHIR to support this interoperability need. • See CDA and CCDA projects in the Interoperability Proving Ground.	

Unique Device Identification

Interoperability Need: Defining a Globally Unique Device Identifier

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Unique device identifier as defined by the Food and Drug Administration at 21 CFR 830.3	Final	Production	●○○○○	Yes	Free	N/A
Implementation Specification	HL7 Harmonization Pattern for Unique Device Identifiers	In Development	Pilot	●○○○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Per the FDA, Unique Device Identification system will be phased in over several years, with the final compliance date of September, 2020. • Compliance date for UDI of implantable, life supporting and life sustaining devices was 9/24/2015. These data are available at http://accessgudid.nlm.nih.gov • The HL7 Harmonization Pattern for UDIs is currently in development, with the next revision release anticipated in February 2018. • See UDI projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Representing Unique Implantable Device Identifiers

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Unique device identifier as defined by the Food and Drug Administration at 21 CFR 830.3	Final	Production	●○○○○	Yes	Free	N/A
Implementation Specification	HL7 Cross-Paradigm Implementation Guide: UDI Pattern, Release 1	Final	Production	●○○○○	No	Free	N/A
Standard	NCPDP SCRIPT Standard, Implementation Guide, Version 2017071	Final	Production	Feedback Requested	No	$	Yes
Standard	NCPDP Telecommunication Standard Implementation Guide, Version F2	Final	Production	Feedback Requested	No	$	-
Implementation Specification	NCPDP Product Identifiers Standard Implementation Guide Version 1.4	Final	Production	Feedback Requested	No	$	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Per the FDA, Unique Device Identification system will be phased in over several years, with the final compliance date of September, 2020. • Compliance date for UDI of implantable, life supporting and life sustaining devices was 9/24/2015. These data are available at http://accessgudid.nlm.nih.gov • HL7 Cross-Paradigm Implementation Guide: UDI Pattern, Release 1 - will be updated with HL7 FHIR Releases. • See UDI projects in the Interoperability Proving Ground.	• Feedback requested.

Interoperability Need: Transmitting a Unique Device Identifier

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Unique device identifier as defined by the Food and Drug Administration at 21 CFR 830.3	Final	Production	●○○○○	Yes	Free	N/A
Implementation Specification	HL7 Harmonization Pattern for Unique Device Identifiers	In Development	Pilot	●○○○○	No	Free	N/A

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Value Set(s) and Starter Set(s):
• Per the FDA, Unique Device Identification system will be phased in over several years, with the final compliance date of September, 2020. • Compliance date for UDI of implantable, life supporting and life sustaining devices was 9/24/2015. These data are available at http://accessgudid.nlm.nih.gov	• Feedback requested.

• The HL7 Harmonization Pattern for UDIs is currently in development. • See UDI projects in the Interoperability Proving Ground.	

Section III: Standards and Implementation Specifications for Services/Transport/Exchange

"Push" Exchange

Interoperability Need: An Unsolicited "Push" of Clinical Health Information to a Known Destination and Information System User

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	Direct (Applicability Statement for Secure Health Transport v1.2)	Final	Production	●●●●○	Yes	Free	Yes
Standard	IHE-XDR (Cross-Enterprise Document Reliable Interchange)	Final	Production	●●●●●	Yes	Free	Yes
Implementation Specification	IG for Direct Edge Protocols	Final	Production	●●○○○	Yes	Free	Yes
Implementation Specification	IG for Delivery Notification in Direct	Final	Production	●●●○○	Yes	Free	Yes
Implementation Specification	XDR and XDM for Direct Messaging Specification	Final	Production	●●●●○	Yes	Free	Yes
Implementation Specification	ITU H.810, H.811, H.812, and H.813	Final	Production	●○○○○	No	Free	Yes
Emerging Implementation Specification	*Implementation Guide for Expressing Context in Direct Messaging v1.1*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• "Direct" standard is based upon the underlying standard: Simple Mail Transfer Protocol (SMTP) RFC 5321 and for security uses Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, RFC 5751. • For Direct, interoperability may be dependent on the establishment of "trust"	• **System Authentication** – The information and process necessary to authenticate the systems involved. • **Recipient Encryption** – the message and health information are encrypted for the intended user.

between two parties and may vary based on the trust community(ies) to which parties belong. The leading trust communities to enable communication amongst the most users include DirectTrust (for provider messaging and consumer-mediated exchange) and NATE (for consumer-mediated exchange). • Direct is not currently supported by a formal SDO but is actively maintained and updated by the Direct Community. • The ITU implementation specifications are Continua Design Guidelines, developed to provide a suite of open industry standards and specifications that provide several means to end-to-end interoperability between personal medical devices and health information systems. Unrestricted access to the implementation specification: http://www.pchalliance.org/continua-design-guidelines • See Direct and IHE projects in the Interoperability Proving Ground.	• **Sender Signature** – details that are necessary to identity of the individual sending the message. • **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Patient Consent Information** – Identifies the patient consent information that may be required before data can be accessed. o May be required to authorize any exchange of patient information. o May be required to authorize access and use of patient information. o May be required to be sent along with disclosed patient information to advise the receiver about policies to which end users must comply. • **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user.

Interoperability Need: An Unsolicited "Push" of Clinical Health Information to a Known Destination Between Systems

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	SOAP-Based Secure Transport Requirements Traceability Matrix (RTM) version 1.0 specification	Final	Production	●●●○○	Yes	Free	Yes
Standard	Direct (Applicability Statement for Secure Health Transport v1.2)	Final	Production	●●○○○	Yes	Free	Yes
Standard	HL7 Fast Healthcare Interoperability Resources (FHIR), DSTU 2	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	eHealth Exchange Specification: Messaging Platform	Final	Production	●●●○○	No	Free	Yes
Implementation Specification	eHealth Exchange Specification: Authorization Framework	Final	Production	●●●○○	No	Free	Yes
Implementation Specification	eHealth Exchange Specification: Document Submission	Final	Production	●●●○○	No	Free	Yes

Implementation Specification	IHE-XDR (Cross-Enterprise Document Reliable Interchange)	Final	Production	●●●●○	No	Free	Yes
Emerging Standard	*HL7 Fast Healthcare Interoperability Resources (FHIR)*	*Final*	*Production*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**
• The IHE-XDR implementation specification is based upon the underlying standards: SOAP v2, and OASIS ebXML Registry Services 3.0. • The eHealth Exchange Specification: Authorization Framework implementation specification is based upon the underlying standards: SAML v1.2, XSPAv1.0, and WS-1.1. • "Direct" standard is based upon the underlying standard: Simple Mail Transfer Protocol (SMTP) RFC 5321 and for security uses Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, RFC 5751. • For Direct, interoperability may be dependent on the establishment of "trust" between two parties and may vary based on the trust community(ies) to which parties belong. The leading trust communities to enable communication amongst the most users include DirectTrust (for provider messaging and consumer-mediated exchange) and NATE (for consumer-mediated exchange). • The reference to FHIR for this interoperability need is in relation to the transport services that are conformant to the "RESTful FHIR API". • FHIR Resources are in various stages of maturity. Please refer to the FHIR website for updates on specific profiles and their progress. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • See FHIR, Direct and IHE projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Medical Device Communication to Other Information Systems/Technologies

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ITU H.810, H.811, H.812, and H.813	Final	Production	●○○○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**
• These ITU standards are Continua Design Guidelines, developed to provide a suite of open industry standards and specifications that provide several means to end-to-end interoperability between personal medical devices and health information systems. Unrestricted access to the implementation specification: http://www.pchalliance.org/continua-design-guidelines	• **System Authentication** - The information and process necessary to authenticate the systems involved. • **User Details** - identifies the end user who is accessing the data. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Push Communication of Vital Signs from Medical Devices

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	IEEE 11073-10101-2004 - Health informatics -- Point-of-care medical device communication -- Part 10101: Nomenclature	Final	Production	●●●○○	No	$	Yes[$]
Implementation Specification	IHE-PCD (Patient Care Device Profiles)	Final	Production	●●○○○	No	Free	Yes
Implementation Specification	ITU H.810, H.811, H.812, H812.5 and H.813	Final	Production	●●●○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• ISO/IEEE 11073 is a family of standards for various medical devices. • The IEEE1073 Nomenclature is recognized in the IHE/HL7 record set. • The ITU implementation specifications are Continua Design Guidelines, developed to provide a suite of open industry standards and specifications that provide several means to end-to-end interoperability between personal medical devices and health information systems. Unrestricted access to the implementation specification: http://www.pchalliance.org/continua/products/design-guidelines.	• Feedback requested.

Interoperability Need: Remote Patient Monitoring to Support Chronic Condition Management, Patient Education, and Patient Engagement

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ITU H.810, H.811, H.812, H812.5, and H.813	Final	Production	●●●○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• These ITU standards are Continua Design Guidelines, developed to provide a suite of open industry standards and specifications that provide several means to end-to-end interoperability between personal medical devices and health information systems. Unrestricted access to the implementation specification: http://www.pchalliance.org/continua-design-guidelines	• **System Authentication** - The information and process necessary to authenticate the systems involved. • **User Details** - identifies the end user who is accessing the data. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Interoperability Need: Representing Path Traversal Expressions							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Emerging Standard	*HL7Fast Healthcare Interoperability Resources (FHIR) – FluentPath, STU 1, Release 1*	Balloted Draft	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See FHIR Projects in the Interoperability Proving Ground.	• Feedback requested.

Clinical Decision Support Services

Interoperability Need: Providing Patient-Specific Assessments and Recommendations Based on Patient Data for Clinical Decision Support							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Standard	HL7 Version 3 Standard: Decision Support Service, Release 2.	Balloted Draft	Pilot	●○○○○	No	Free	No
Implementation Specification	HL7 Implementation Guide: Decision Support Service, Release 1.1, US Realm, Draft Standard for Trial Use	Balloted Draft	Pilot	●○○○○	No	Free	No
Standard	HL7 FHIR Profile: Quality Improvement Core (QI Core), Release 1, STU 3	Balloted Draft	Pilot	●●○○○	No	Free	No
Standard	HL7 Cross-Paradigm Specification: Clinical Quality Language (CQL), Release 1, STU Release 2	Balloted Draft	Pilot	●●●○○	No	Free	Yes
Emerging Implementation Specification	*CDS Hooks Services*	*Balloted Draft*	*Pilot*	●●○○○	*No*	*Free*	*Yes*
Emerging Implementation Specification	*IHE-GAO (Guideline Appropriate Ordering)*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• FHIR Resources are in various stages of maturity. Please refer to the FHIR website for updates on specific profiles and their progress. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • See FHIR & IHE projects in the Interoperability Proving Ground.	• **System Authentication** - The information and process necessary to authenticate the systems involved. • **Recipient Encryption** - the message and health information are encrypted for the intended user. • **Sender Signature** – details that are necessary to identity of the individual sending the message. • **Secure Communication** – create a secure channel for client-to- serve and server-

	to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user.

Interoperability Need: Retrieval of Contextually Relevant, Patient-Specific Knowledge Resources from Within Clinical Information Systems to Answer Clinical Questions Raised by Patients in the Course of Care

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application ("Infobutton"), Knowledge Request, Release 2	Final	Production	●●●●○	Yes	Free	No
Implementation Specification	HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4	Final	Production	●●●●○	Yes	Free	No
Implementation Specification	HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1	Final	Production	●●●●○	Yes	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Feedback requested.	• Feedback requested.

Consumer Access/Exchange of Health Information

Interoperability Need: Patient Exchanging Secure Messages with Care Providers

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	Direct (Applicability Statement for Secure Health Transport v1.2)	Final	Production	●●○○○	Yes	Free	Yes
Emerging Implementation Specification	*HL7 Fast Healthcare Interoperability Resources (FHIR) STU Release 3*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• To learn more about Patient Portals and their usage, see the Patient Engagement	• **System Authentication** – The information and process necessary to authenticate

Playbook. • See FHIR, Direct, Patient Portal, API, and Open API projects in the Interoperability Proving Ground. • "Direct" standard is based upon the underlying standard: Simple Mail Transfer Protocol (SMTP) RFC 5321 and for security uses Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, RFC 5751. • For Direct, interoperability may be dependent on the establishment of "trust" between two parties and may vary based on the trust community(ies) to which parties belong. The leading trust communities to enable communication amongst the most users include DirectTrust (for provider messaging and consumer-mediated exchange) and NATE (for consumer-mediated exchange). • Direct is not currently supported by a formal SDO but is actively maintained and updated by the Direct Community. • Current Procedural Terminology (CPT) Consumer Friendly Descriptors (CFDs) may be used when data is being exchanged between patients and providers. • When using the SMART on FHIR model, the authentication model uses OAuth2. Except for "Secure Communication", the security patterns listed do not apply.	the systems involved. • **User Details** – identifies the end user who is accessing the data. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** – Identifies the purpose for the transaction. • **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user. • **Secure Communication** – create a secure channel for client-to-server and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.

Interoperability Need: Push Patient-Generated Health Data into Integrated EHR

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	Direct (Applicability Statement for Secure Health Transport v1.2)	Final	Production	●●○○○	Yes	Free	Yes
Emerging Implementation Specification	*HL7 Fast Healthcare Interoperability Resources (FHIR) STU Release 3*	*Balloted Draft*	*Pilot*	●○○○○	*Yes*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• To learn more about Patient-Generated Health Data and its usage, see the Patient Engagement Playbook, as well as ONC's Patient-Generated Health Data webpage. • Current Procedural Terminology (CPT) Consumer Friendly Descriptors (CFDs) may be used, as appropriate, when pushing patient-generated health data into integrated EHRs. • A draft white paper for a Patient-Generated Health Data policy framework, created under an ONC contract, is available for review. A final version will be published in early 2018. • The SMART on FHIR Project is working in this area, and may have additional implementation guidance, as well as a list of applications supporting this interoperability need. • See FHIR, Direct, Patient Portal, API, and Open API projects in the Interoperability Proving Ground.	• **System Authentication** – The information and process necessary to authenticate the systems involved. • **User Details** – identifies the end user who is accessing the data. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** – Identifies the purpose for the transaction. • **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user. • **Query Request ID** – Query requesting application assigns a unique identifier for each query request in order to match the response to the original query. • **Secure Communication** – create a secure channel for client-to-server and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.

• "Direct" standard is based upon the underlying standard: Simple Mail Transfer Protocol (SMTP) RFC 5321 and for security uses Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, RFC 5751. • For Direct, interoperability may be dependent on the establishment of "trust" between two parties and may vary based on the trust community(ies) to which parties belong. The leading trust communities to enable communication amongst the most users include DirectTrust (for provider messaging and consumer-mediated exchange) and NATE (for consumer-mediated exchange). • Direct is not currently supported by a formal SDO but is actively maintained and updated by the Direct Community. • When using the SMART on FHIR model, the authentication model uses OAuth2. Except for "Secure Communication", the security patterns listed do not apply.	

Interoperability Need: Remote Patient Authorization and Submission of EHR Data for Research

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Emerging Implementation Specification	*HL7 Fast Healthcare Interoperability Resources (FHIR) STU Release 3*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• See Sync for Science and Sync for Genes for more details about the research project use case that pertains to this interoperability need.
• The Kantara Initiative's UMA (User Managed Access) Work Group project's use case is designed to develop specifications that allow individual control of authorized data sharing and service access to promote interoperability in support of this interoperability need.
• The reference to FHIR for this interoperability need is in relation to the transport services that are conformant to the RESTful FHIR API.
• See FHIR , API, and Open API projects in the Interoperability Proving Ground.
• Current Procedural Terminology (CPT) Consumer Friendly Descriptors (CFDs) may be used when data is being exchanged between patients and providers.
• When using the SMART on FHIR model, the authentication model uses OAuth2. The other security patterns listed do not apply.
	• **System Authentication** – The information and process necessary to authenticate the systems involved.
	• **User Details** – identifies the end user who is accessing the data.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Patient Consent Information** – Identifies the patient consent information that may be required before data can be accessed.
	  ○ May be required to authorize any exchange of patient information
	  ○ May be required to authorize access and use of patient information.
	  ○ May be required to be sent along with disclosed patient information to advise the receiver about policies to which end users must comply.
	• **Purpose of Use** – Identifies the purpose for the transaction.
	• **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user.

Interoperability Need: View, Download, and Transmit Data from EHR

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	Direct (Applicability Statement for Secure Health Transport v1.2)	Final	Production	●●○○○	Yes	Free	Yes
Implementation Specification	HL7 Fast Healthcare Interoperability Resources (FHIR) STU 2, Argonaut Data Query Implementation Guide	Balloted Draft	Production	●●●○○	No	Free	Yes Yes Yes
Emerging Implementation Specification	*HL7 Fast Healthcare Interoperability Resources (FHIR) STU Release 3*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• To learn more about Patient Portals and their usage, see the Patient Engagement Playbook.
• See FHIR, Direct, Patient Portal, API, and Open API projects in the Interoperability Proving Ground.
• "Direct" standard is based upon the underlying standard: Simple Mail Transfer Protocol (SMTP) RFC 5321 and for security uses Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, RFC 5751.
• For Direct, interoperability may be dependent on the establishment of "trust" between two parties and may vary based on the trust community(ies) to which parties belong. The leading trust communities to enable communication amongst the most users include DirectTrust (for provider messaging and consumer-mediated exchange) and NATE (for consumer-mediated exchange).
• Direct is not currently supported by a formal SDO but is actively maintained and updated by the Direct Community.
• Current Procedural Terminology (CPT) Consumer Friendly Descriptors (CFDs) may be used when data is being exchanged between patients and providers.
• The reference to FHIR for this interoperability need is in relation to the transport services that are conformant to the RESTful FHIR API.
• When using the SMART on FHIR model, the authentication model uses OAuth2. Except for "Secure Communication", the security patterns listed do not apply.
	• **System Authentication** – The information and process necessary to authenticate the systems involved.
	• **User Details** – identifies the end user who is accessing the data.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** – Identifies the purpose for the transaction.
	• **Patient Consent Information** – Identifies the patient consent information that may be required before data can be accessed.
	  ○ May be required to authorize any exchange of patient information.
	  ○ May be required to authorize access and use of patient information.
	  ○ May be required to be sent along with disclosed patient information to advise the receiver about policies to which end users must comply.
	• **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user.
	• **Secure Communication** – create a secure channel for client-to-server and server-to-server communication.
	• **Query Request ID** – Query requesting application assigns a unique identifier for each query request in order to match the response to the original query.
	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery.

Image Exchange

Interoperability Need: Exchanging Imaging Documents Outside a Specific Health Information Exchange Domain

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	DICOMweb™	Final	Production	Feedback requested	No	Free	No
Implementation Specification	IHE-Cross Community Access for Imaging (XCA-I)	Final	Pilot	●○○○○	No	Free	Yes
Implementation Specifications	the combination of IHE-XCPD (Cross-Community Patient Discovery) and IHE-PIX (Patient Identifier Cross-Reference)	Final	Production	●●●●○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• IHE-PIX and IHE-XCPD are used for the purposes of patient matching and to support this interoperability need. • See IHE projects in the Interoperability Proving Ground.	• **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos).

Interoperability Need: Exchanging Imaging Documents Within a Specific Health Information Exchange Domain

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Standard	DICOMweb™	Final	Production	Feedback requested	No	Free	No
Implementation Specification	IHE-Cross Enterprise Document Sharing for Images (XDS-I.b)	Final	Pilot	●○○○○	No	Free	Yes
Implementation Specification	IHE-PDQ (Patient Demographic Query)	Final	Production	●●●●○	No	Free	Yes
Implementation Specification	IHE-PIX (Patient Identifier Cross-Reference)	Final	Production	●●●●○	No	Free	Yes
Emerging Implementation Specification	IHE - Patient Identifier Cross-reference for Mobile (PIXm)	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Emerging Implementation Specification	*IHE-MHD-I (Mobile Access to Health Documents for Imaging)*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• IHE-PIX and IHE-PDQ are used for the purposes of patient matching and to support this interoperability need. • See IHE projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Healthcare Directory, Provider Directory

Interoperability Need: Listing of Providers for Access by Potential Exchange Partners

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	Validated Healthcare Directory Implementation Guide Home	Balloted Draft	Pilot	●○○○○	No	Free	Yes
Implementation Specification	IHE-IT Infrastructure Technical Framework Supplement, Healthcare Provider Directory (HPD), Trial Implementation	Balloted Draft	Pilot	●○○○○	No	Free	Yes
Implementation Specification	HL7 Argonaut Provider Directory Implementation Guide Version 1.0.0	Balloted Draft	Production	●●○○○	No	Free	Yes
Implementation Specification	IHE Mobile Care Services Discovery (mCSD)	Balloted Draft	Pilot	Feedback Requested	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The IHE IT Infrastructure Technical Framework Supplement, Healthcare Provider Directory (HPD), Trial Implementation was proposed, but not adopted for CEHRT	• **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user.

2015. The Health IT community has recognized the value of the underlying data elements and structure of that standard. The standard has met with limited adoption due to several concerns. • FHIR Resources are in various stages of maturity. Please refer to the FHIR website for updates on specific profiles and their progress. The FHIR Maturity Model and each of the levels is described on the HL7 wiki. • See IHE and FHIR projects in the Interoperability Proving Ground.	

Patient Identification Management

Interoperability Need: Exchanging Patient Identification Management Within a Community

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE-PDQ (Patient Demographic Query)	Final	Production	●●●●●	No	Free	Yes
Implementation Specification	IHE-PIX (Patient Identifier Cross-Reference)	Final	Production	●●●●●	No	Free	Yes
Implementation Specification	IHE – XCPD (Cross Community Patient Discovery)	Final	Production	●●●●●	No	Free	Yes
Emerging Implementation Specification	*IHE - Patient Identifier Cross-reference PIX for Mobile (PIXm)*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See Section II: Patient Identification Management for more information about the HL7 2.5.1 ADT messaging standard and information about patient identity proofing.	• Feedback requested.

Public Health Exchange

Interoperability Need: Transport for Immunization Submission and Query/Response							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	CDC-EHR-IIS Interoperability Enhancement Project Transport Layer Protocol Recommendation Formal Specification, Version 1.2	Final	Production	●●●●○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**
• Feedback requested.	• Feedback requested.

Publish and Subscribe

Interoperability Need: Publish and Subscribe Message Exchange							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	eHealth Exchange Specification: Health Information Event Messaging Production Specification	Final	Production	●○○○○	No	Free	No
Emerging Implementation Specification	*IHE Document Metadata Subscription (DSUB), Trial Implementation*	*Balloted Draft*	*Pilot*	●●○○○	*No*	*Free*	*Yes*

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**
• The listed eHealth Exchange Specification will be deprecated in the future in favor of the emerging IHE DSUB specification and/or the equivalent FHIR profile. • See IHE projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Assertion Builder** – define processing logic for identity, authorization and attribute statements. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Query

Interoperability Need: Data Element Based Query for Clinical Health Information

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 Argonaut Data Query Implementation Guide Version 1.0.0	Balloted Draft	Production	●●○○○	No	Free	Yes Yes
Emerging Implementation Specification	*IHE Mobile Cross-Enterprise Document Data Element Extraction (mXDE) Profile*	*Balloted Draft*	*Pilot*	*Feedback Requested*	*No*	*Free*	*No*
Emerging Implementation Specification	*IHE Query for Existing Data for Mobile (QEDm)*	*Balloted Draft*	*Pilot*	*Feedback Requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• The reference to FHIR for this interoperability need is in relation to the transport services that are conformant to the "RESTful FHIR API".
• Note that the maturity level of FHIR resources may vary. The FHIR Maturity Model and each of the levels is described on the HL7 wiki.
• See FHIR projects in the Interoperability Proving Ground.
	• **System Authentication** - The information and process necessary to authenticate the systems involved
	• **User Details** - identifies the end user who is accessing the data.
	• **User Role** – identifies the role asserted by the individual initiating the transaction.
	• **Purpose of Use** - Identifies the purpose for the transaction.
	• **Patient Consent Information** - Identifies the patient consent information that may be required before data can be accessed.
	  ○ May be required to authorize any exchange of patient information.
	  ○ May be required to authorize access and use of patient information.
	  ○ May be required to be sent along with disclosed patient information to advise the receiver about policies to which end users must comply.
	• **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user.
	• **Query Request ID** - Query requesting application assigns a unique identifier for each query request in order to match the response to the original query.

Interoperability Need: Query for Documents Outside a Specific Health Information Exchange Domain							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	IHE-XCA (Cross-Community Access)	Final	Production	●●●●○	No	Free	Yes
Implementation Specification	IHE-XCPD (Cross-Community Patient Discovery)	Final	Production	●●●●○	No	Free	Yes
Implementation Specification	IHE-PIX (Patient Identifier Cross-Reference)	Final	Production	●●●●○	No	Free	Yes
Implementation Specification	eHealth Exchange Specification: Patient Discovery	Final	Production	●●●○○	No	Free	Yes
Implementation Specification	eHealth Exchange Specification: Messaging Platform	Final	Production	●●●○○	No	Free	Yes
Implementation Specification	eHealth Exchange Specification: Authorization Framework	Final	Production	●●●○○	No	Free	Yes
1-Implementation Specification	eHealth Exchange Specification: Query for Documents	Final	Production	●●●○○	No	Free	Yes
1-Implementation Specification	eHealth Exchange Specification: Retrieve Documents	Final	Production	●●●○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	**Applicable Security Patterns for Consideration:**
• IHE-PIX and IHE-XCPD are used for the purposes of patient matching and to support this interoperability need. • While IHE-PIX and IHE-XCPD are best-available standards at this time, the current best-available standards may be insufficient to meet interoperability needs with sufficient accuracy. • See IHE projects in the Interoperability Proving Ground.	• **System Authentication** - The information and process necessary to authenticate the systems involved. • **User Authentication** – The information and process necessary to authenticate the end user. • **User Details** - identifies the end user who is accessing the data. • **User Role** - identifies the roles and clearances asserted by the individual initiating the transaction for purposes of authorization. E.g., the system must verify the

	initiator's claims and match them against the security labels for the functionalities that the user attempts to initiate and the objects the user attempts to access.
	• **Purpose of Use** - Identifies the purpose for the transaction, and for the purposes for which the end user intends to use the accessed objects.
	• **Patient Consent Information** - Identifies the patient consent information that may be required before data can be accessed.
	  ○ May be required to authorize any exchange of patient information.
	  ○ May be required to authorized access and use of patient information.
	  ○ May be required to be sent along with disclosed patient information to advise the receiver about policies to which end users must comply.
	• **Query Request ID** - Query requesting application assigns a unique identifier for each query request in order to match the response to the original query.
	• **Security Labeling** – the health information is labeled with security metadata necessary for access control by the end user.

Interoperability Need: Query for Documents Within a Specific Health Information Exchange Domain

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE-XDS (Cross-enterprise document sharing)	Final	Production	●●●●●	No	Free	Yes
Implementation Specification	IHE-PDQ (Patient Demographic Query)	Final	Production	●●●●●	No	Free	Yes
Implementation Specification	IHE-PIX (Patient Identifier Cross-Reference)	Final	Production	●●●●●	No	Free	Yes
Emerging Implementation Specification	*IHE-MHD (Mobile Access to Health Documents)*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*Yes*
Emerging Implementation Specification	*IHE-PIXm (Patient Identifier Cross-Reference for Mobile)*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*
Emerging Implementation Specification	*IHE-PDQm (Patient Demographics Query for Mobile)*	*Balloted Draft*	*Pilot*	●○○○○	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:

• IHE-PIX and IHE-PDQ are used for the purposes of patient matching and to support this interoperability need along with IHE-XDS. • The MHD Supplement Revision 2.2 published in April 2016 is based on FHIR DSTU2. • IHE-PIXm and IHE-PDQm are used for the purposes of patient matching and to support this interoperability need along with MHD. • See IHE projects in the Interoperability Proving Ground.	• **Secure Communication** – create a secure channel for client-to- serve and server-to-server communication. • **Secure Message Router** – securely route and enforce policy on inbound and outbound messages without interruption of delivery. • **Authentication Enforcer** – centralized authentication processes. • **Authorization Enforcer** – specifies access control policies. • **Credential Tokenizer –** encapsulate credentials as a security token for reuse (e.g., – SAML, Kerberos). • **Message Interceptor Gateway** – provide a single entry point solution for centralization of security enforcement for incoming and outgoing XML WebService messages. • **System Authentication** - The information and process necessary to authenticate the systems involved. • **User Authentication** – The identity information and process necessary verify the user's identity. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction. • **Security Labeling** – the health information is labeled with security metadata

Resource Location

Interoperability Need: Care Service Discovery Within the US

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	IHE IT Infrastructure Technical Framework Supplement, Care Services Discovery (CSD), Trial Implementation	Balloted Draft	Pilot	●○○○○	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• See IHE projects in the Interoperability Proving Ground.	• **System Authentication** - The information and process necessary to authenticate the systems involved. • **User Details** - identifies the end user who is accessing the data. • **User Role** – identifies the role asserted by the individual initiating the transaction. • **Purpose of Use** - Identifies the purpose for the transaction.

Section IV: Administrative Standards and Implementation Specifications

Administrative Transactions - Non-Claims

Interoperability Need: Enrollment and Disenrollment in a Health Plan

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ASC X12N/005010X220 Benefit Enrollment and Maintenance (834), August 2006 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 and ASC X12N/005010X220A1 Type 1 Errata to Benefit Enrollment and Maintenance (834), June 2010 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●○○	Yes	$	Yes
Implementation Specification	ASC X12N/005010X307 Health Insurance Exchange: Enrollment (834), January 2013, as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●○○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link.
- This standard and the transaction were adopted under the Health Insurance Portability Act of 1996 (HIPAA) to increase efficiency in the health care system by reducing the use of paper and increasing the exchange of health care information electronically. This information is often maintained in provider practice management and billing systems but duplicates information in electronic health records.
- Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated.
- There are two versions of the enrollment transaction in use by industry today. One is the adopted transaction exchanged between a covered health plan and the

Applicable Security Patterns for Consideration:

- All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

employer, which is not a covered entity. The adoption rate is unknown. The other version, referred to as the HIX, has not been adopted by the federal government, but is used by the issuers participating in the federal marketplace or health insurance exchanges created by the Affordable Care Act. It includes data elements necessary to complete that enrollment process. • Additional information is available on testing, and the full cost on any of the X12 transactions. • For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set. ASETT is the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions.	

Interoperability Need: Health Care Eligibility Benefit Inquiry and Response

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ASC X12N/005010X279 Health Care Eligibility Benefit Inquiry and Response (270/271), April 2008 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 and ASC X12N/005010X279A1 Type 1 Errata to Health Care Eligibility Inquiry and Response (270/271), June 2010 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●●●	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link. • This standard and the transaction were adopted under the Health Insurance Portability Act of 1996 (HIPAA) to increase efficiency in the health care system by reducing the use of paper and increasing the exchange of health care information electronically. This information is often maintained in provider practice management and billing systems but duplicates information in electronic health records.	• All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

• Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated. • Additional information is available on testing, and the full cost on any of the X12 transactions. ASETT is the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions. • For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set.	

Interoperability Need: Health Care Eligibility Benefit Inquiry and Response for Retail Pharmacy Coverage

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	NCPDP Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2010	Final	Production	●●●●●	Yes	$	Yes
Implementation Specification	NCPDP Telecommunication Standard, Implementation Guide, Version F2, March 2018 and Equivalent Batch Standard Implementation Guide, Version 15	Final	Pilot	●○○○○	No	$	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link. • This standard and the transaction were adopted under the Health Insurance Portability Act of 1996 (HIPAA) to increase efficiency in the health care system by reducing the use of paper and increasing the exchange of health care information electronically. This information is often maintained in provider practice management and billing systems but duplicates information in electronic health records. • Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated. • Costs to access the NCPDP standards are based on membership status. NCPDP's Standards Matrix is available as a reference providing a high-level overview of the	• All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

latest version/release and/or the most commonly used of NCPDP standards and implementation guides, as well as NCPDP's Data Dictionary and External Code List. • The Telecommunication Standard Implementation Guide Version F2 has been recommended for adoption under HIPAA by NCVHS. NCPDP is in the investigative stage of providing a test tool for this version.	

Administrative Transactions to Financial Exchanges

Interoperability Need: Electronic Funds Transfer for Payments to Health Care Providers

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	NACHA Operating Rules, Appendix One and Three ACH File Exchange Specifications; ACH Record Format Specifications, Subpart 3.1.8 Sequence of Records for CCD Entries; and Data content in CCD Addenda Record: ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, "Health Care Claim Payment/Advice (835), April 2006: Section 2.4: 835 Segment Detail: "TRN"	Final	Production	●●●○○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• File testing is done between the banks and their originators of the ACH files, between the banks and the ACH Operators and for the software vendors with the ACH Operators. Testing for a new originator is done with the bank before they originate their first file. Testing between the banks and the ACH Operators is done when there is a new application – currently a lot of testing is being done between the banks and the ACH Operators for Same Day ACH Debits (to be implemented in September 2017). If a bank changes ACH processing software or hires a third-party vendor, testing will be done between the bank and the ACH Operator. • Because only the current version of an ACH file format is allowed through the ACH Network, the originating bank reviews all files to make sure that the formatting is correct before they send the files to the ACH Operators. The ACH Operators also review all files to make sure that the mandatory fields within the ACH file are formatted correctly – if they are not the files are returned to the originating bank. Both the originating bank and the ACH Operators are looks at the files to make sure that the files are syntactically correct. • ACH Network is an electronic funds transfer system governed by the NACHA Operating Rules, which provides for interbank clearing of electronic entries for participating financial institutions.	• All covered entities are required to meet HIPAA security and privacy requirements in order for Electronic Data Interchange (EDI) to occur. • For Automated Clearing House (ACH) Network risks and enforcement, one can refer to NACHA's ACH Network Risk and Enforcement Topics and 2017 NACHA Operating Rules & Guidelines.

Interoperability Need: Health Care Payment and Remittance Advice

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ASC X12N/005010X221 Health Care Claim Payment/Advice (835), April 2006 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 and ASC X12N/005010X221A1 Type 1 Errata to Health Care Claim Payment/Advice (835), June 2010 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●○○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link.
- Adoption of standards to increase the efficiency of the health care system was required by the Health Insurance Portability Act of 1996 (HIPAA). This version of the standard was adopted in 2009, and compliance was required by January 2012. The purpose of the electronic standard transactions was to improve efficiency in the health care system by reducing the use of paper and increasing the electronic exchange of health care information.
- Challenges with this transaction may occur when the remittance information does not match the claim or the payment.
- Additional information is available on testing, and the full cost on any of the X12 transactions. ASETT is the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions.
- For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set.
- Pharmacy providers will receive the X12 835 remittance advice transaction with their payments, and NCPDP offers specific guidance on how the X12 835 remittance advice should be mapped in response to the NCPDP D.0 claim transaction to maximize reconciliation.

Applicable Security Patterns for Consideration:

- All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

Interoperability Need: Health Plan Premium Payments for Covered Members

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ASC X12N/005010X218 Payroll Deducted and Other Group Premium Payment for Insurance Products (820), February 2007 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●○○○	Yes	$	Yes
Implementation Specification	ASC X12N/005010X306 Health Insurance Exchange Related Payments (820), January 2013 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	Feedback Requested	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link.
- This standard and the transaction were adopted under the Health Insurance Portability Act of 1996 (HIPAA) to increase efficiency in the health care system by reducing the use of paper and increasing the exchange of health care information electronically. This information is often maintained in provider practice management and billing systems but duplicates information in electronic health records.
- Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated.
- Additional information is available on testing, and the full cost on any of the X12 transactions. ASETT is the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions
- For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set.

Applicable Security Patterns for Consideration:

- All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

Administrative Transactions to Support Clinical Care

Interoperability Need: Health Care Attachments to Support Claims, Referrals and Authorizations

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ASC X12N/006020X315 Health Care Services Request for Review and Response (278), September 2014 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Pilot	●○○○○	No	$	No
Implementation Specification	ASC X12N/006020X313 Health Care Claim Request for Additional Information (277), September 2014 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Pilot	●○○○○	No	$	No
Implementation Specification	ASC X12N/006020X316 Additional Information to Support a Health Care Services Review (275), September 2014 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Pilot	●○○○○	No	$	No
Implementation Specification	ASC X12C/005010X231 Implementation Acknowledgment for Health Care Insurance (999), June 2007 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 and ASC X12C/005010X231A1 Type 1 Errata to Implementation Acknowledgment for Health Care Insurance (999), June 2010 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●●○	No	$	No
Implementation Specification	ASC X12N/006020X290 Implementation Acknowledgment for Health Care Insurance (999), September 2013 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Pilot	●○○○○	No	$	No
Implementation Specification	HL7 CDA® R2 Attachment Implementation Guide: Exchange of C-CDA Based Documents, Release 1 - US Realm	Balloted Draft	Pilot	●○○○○	No	$	No
Implementation Specification	HL7 CDA R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes (US Realm) Draft Standard for Trial Use Release 2.1	Balloted Draft	Pilot		No	$	No

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	HL7 Implementation Guide for CDA® Release 2: Additional CDA R2 Templates - Clinical Documents for Payers – Set 1, Release 1.1 (US Realm)	Final	Pilot	●○○○○	No	$	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The standards for attachments to support claims and other administrative transactions have not been adopted for use, though the original HIPAA legislation required their adoption, and the Affordable Care Act reiterated the requirement. • A proposed rule was published in 2005, and a final rule was released in 2006, and then withdrawn. • There are at least two provider/payer partners who have implemented the attachment standards successfully, on a voluntary basis, following a pilot project in 2004. • CMS provides additional information about the HIPAA administrative simplification provisions.	• Feedback requested.

Interoperability Need: Referral Certification and Authorization for Pharmacy Transactions

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	NCPDP Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2010	Final	Production	●●●○○	Yes	$	Yes
Implementation Specification	NCPDP SCRIPT Standard Implementation Guide, Version 2013101	Final	Production	●●○○○	Yes	$	No
Implementation Specification	NCPDP Telecommunication Standard, Implementation Guide, Version F2, March 2018	Final	Pilot	●○○○○	No	$	No
Implementation Specification	NCPDP SCRIPT Standard, Implementation Guide, Version 201707	Final	Pilot	●○○○○	No	$	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Costs for access to the NCPDP standards are based on membership. NCPDP's Standards Matrix is available as a reference providing a high-level overview of the latest version/release and/or the most commonly used of NCPDP standards and implementation guides, as well as NCPDP's Data Dictionary and External Code List.	• Feedback requested.

• The Telecommunication Standard Implementation Guide Version F2 and SCRIPT Standard Version 2017071 have been recommended for adoption under HIPAA by NCVHS. • NCPDP is in the investigative stage of providing a test tool for the Telecommunication Standard, and has a testing tool available for the SCRIPT Standard Version 2017071.	

Interoperability Need: Referral Certification and Authorization Request and Response for Dental, Professional and Institutional Services

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ASC X12N/005010X217 Health Care Services Review—Request for Review and Response (278), May 2006 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●○○○○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link. • Adoption of standards to increase the efficiency of the health care system was required by the Health Insurance Portability Act of 1996 (HIPAA). This version of the standard was adopted in 2009, and compliance was required by January 2012. The purpose of the electronic standard transactions was to improve efficiency in the health care system by reducing the use of paper and increasing the electronic exchange of health care information. • Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated. • Additional information is available on testing, and the full cost on any of the X12 transactions. ASETT is the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions. • For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set.	• All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

CMS Interoperability Standards for Provider to Provider Communication

Interoperability Need: Durable Medical Equipment/Home Health Agency Document Request

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	CMS EMDI Implementation Guide Section 4.1.2 and Appendix B	In Development	Pilot	Feedback requested	No	Free	No
Implementation Specification	CMS EMDI Implementation Guide Section 5.1.5.4	In Development	Pilot	Feedback requested	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:

- Organizations may use an internal (native) or external EHR/document management system that provides the following capabilities:
  - Send and receive patient records to providers with electronic referrals.
  - Send and receive documents related to the use cases using secure messaging.
  - Integrate information from other systems, as required, to provide complete documentation.
  - Send multiple documents, as necessary, to meet the use cases.
  - Create metadata where appropriate.
  - Ensure that all documents clearly indicate the patient and provider responsible for each item of documentation created or signed off by a different provider.
  - Clearly indicate the document type (e.g. Mime type) for each document.
  - Provide electronic or digital signature capabilities for all clinical documents.
  - Consume the associated clinical data and integrate it into the patient's medical record.
- Best practices for this interoperability need include including previous treatment attempts in current durable medical equipment request.

Applicable Security Patterns for Consideration:

- Feedback requested.

Interoperability Need: Durable Medical Equipment/Home Health Agency Order Submission

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	CMS EMDI Implementation Guide Section 4.1.1 and Appendix B	In Development	Pilot	Feedback requested	No	Free	No
Implementation Specification	CMS EMDI Implementation Guide Section 5.1.5.1	In Development	Pilot	Feedback requested	No	Free	No

Limitations, Dependencies, and Preconditions for Consideration:

- Organizations may use an internal (native) or external EHR/document management system that provides the following capabilities:
  - Send and receive patient records to providers with electronic referrals.
  - Send and receive documents related to the use cases using secure messaging.
  - Integrate information from other systems, as required, to provide complete documentation.
  - Send multiple documents, as necessary, to meet the use cases.
  - Create metadata where appropriate.
  - Ensure that all documents clearly indicate the patient and provider responsible for each item of documentation created or signed off by a different provider.
  - Clearly indicate the document type (e.g. Mime type) for each document.
  - Provide electronic or digital signature capabilities for all clinical documents.
  - Consume the associated clinical data and integrate it into the patient's medical record.
- Best practices for this interoperability need include including previous treatment attempts in current durable medical equipment request.

Applicable Security Patterns for Consideration:

- Feedback requested.

Interoperability Need: Durable Medical Equipment/Home Health Agency Signature Request

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Emerging Implementation Specification	*CMS EMDI Implementation Guide Section 4.1.3 and Appendix B*	*In Development*	*Pilot*	*Feedback requested*	*No*	*Free*	*No*
Emerging Implementation Specification	*CMS EMDI Implementation Guide Section 5.1.5.7*	*In Development*	*Pilot*	*Feedback requested*	*No*	*Free*	*No*

Limitations, Dependencies, and Preconditions for Consideration:

- Organizations may use an internal (native) or external EHR/document management system that provides the following capabilities:
  - Send and receive patient records to providers with electronic referrals.
  - Send and receive documents related to the use cases using secure messaging.
  - Integrate information from other systems, as required, to provide complete documentation.
  - Send multiple documents, as necessary, to meet the use cases.
  - Create metadata where appropriate.
  - Ensure that all documents clearly indicate the patient and provider responsible for each item of documentation created or signed off by a different provider.
  - Clearly indicate the document type (e.g. Mime type) for each document.
  - Provide electronic or digital signature capabilities for all clinical documents.
  - Consume the associated clinical data and integrate it into the patient's medical record.

Applicable Security Patterns for Consideration:

- Feedback requested.

Health Care Claims and Coordination of Benefits

Interoperability Need: Health Care Claims or Equivalent Encounter Information for Dental Claims

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	ASC X12N/005010X224 ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 and ASC X12N/005010X224A2 Type 1 Errata to Health Care Claim: Dental (837), June 2010 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●●●	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link.
- This standard and the transaction were adopted under the Health Insurance Portability Act of 1996 (HIPAA) to increase efficiency in the health care system by reducing the use of paper and increasing the exchange of health care information electronically. This information is often maintained in provider practice management and billing systems but duplicates information in electronic health records.
- This transaction is also used to conduct coordination of benefits (COB) between entities that agree to do so.
- Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated.
- Additional information is available on testing, and the full cost on any of the X12 transactions. ASETT the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions.
- For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set.

Applicable Security Patterns for Consideration:

- All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

Interoperability Need: Health Care Claims or Equivalent Encounter Information for Institutional Claims							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	ASC X12/N005010X223 Health Care Claim: Institutional (837), May 2006 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 and ASC X12N/005010X223A2 Type 1 Errata to Health Care Claim: Institutional (837), June 2010 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●●●	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link.
- This standard and the transaction were adopted under the Health Insurance Portability Act of 1996 (HIPAA) to increase efficiency in the health care system by reducing the use of paper and increasing the exchange of health care information electronically. This information is often maintained in provider practice management and billing systems but duplicates information in electronic health records.
- This transaction is also used to conduct coordination of benefits between entities that agree to use it between their two organizations.
- Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated.
- Additional information is available on testing, and the full cost on any of the X12 transactions. ASETT the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions.
- For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set.

Applicable Security Patterns for Consideration:

- All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

Interoperability Need: Health Care Claims or Equivalent Encounter Information for Professional Claims							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	ASC X12N/005010X222 Health Care Claim: Professional (837), May 2006 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 and ASC X12N/005010X222A1 Type 1 Errata to Health Care Claim: Professional (837), June 2010 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●●●	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link.
- This standard and the transaction were adopted under the Health Insurance Portability Act of 1996 (HIPAA) to increase efficiency in the health care system by reducing the use of paper and increasing the exchange of health care information electronically. The current version was adopted in 2009, and required for use in 2012. Content from the transactions is often maintained in provider practice management and billing systems but duplicates information in electronic health records.
- Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated.
- Additional information is available on testing, and the full cost on any of the X12 transactions. ASETT the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions.

Applicable Security Patterns for Consideration:

- All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

Interoperability Need: Health Care Claims or Equivalent Encounter Information for Retail Pharmacy Claims							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	NCPDP Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2010	Final	Production	●●●●●	Yes	$	Yes
Implementation Specification	NCPDP Telecommunication Standard, Implementation Guide, Version F2, March 2018 and Equivalent Batch Standard Implementation Guide, Version 15	Final	Pilot	●○○○○	No	$	No
Implementation Specification	NCPDP Batch Standard Medicaid Subrogation Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007	Final	Production	●●●●●	Yes	$	-
Emerging Implementation Specification	*NCPDP Batch Standard Medicaid Subrogation Implementation Guide, Version 10*	*Final*	*Pilot*	*Feedback Requested*	*No*	*$*	-

Limitations, Dependencies, and Preconditions for Consideration:

- The pharmacy telecommunication standard provides a standard format for the electronic submission of third party drug claims and other transactions between pharmacy providers, health plans (payers, insurance companies), third-party administrators, and others with financial responsibility.
- Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), all covered entities – health plans, clearinghouses and covered health care providers are required to use the telecommunication standard for claim and service billing, as well as eligibility verification, predetermination of benefits, and prior authorization. The standard can perform a variety of other functions as well.
- Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated.
- Costs for access to the NCPDP standards are based on membership. NCPDP's Standards Matrix is available as a reference providing a high-level overview of the latest version/release and/or the most commonly used of NCPDP standards and implementation guides, as well as NCPDP's Data Dictionary and External Code List.

Applicable Security Patterns for Consideration:

- All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

Interoperability Need: Health Care Claims or Equivalent Encounter Information for Retail Pharmacy Supplies and Professional Services							
Type	**Standard/Implementation Specification**	**Standards Process Maturity**	**Implementation Maturity**	**Adoption Level**	**Federally Required**	**Cost**	**Test Tool Availability**
Implementation Specification	NCPDP Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2010	Final	Production	●●●●●	Yes	$	Yes
Implementation Specification	ASC X12N/005010X222 Health Care Claim: Professional (837), May 2006 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 and ASC X12N/005010X222A1 Type 1 Errata to Health Care Claim: Professional (837), June 2010 as Type 1 Errata to an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●●●	Yes	$	Yes
Implementation Specification	NCPDP Uniform Healthcare Payer Date Standard Implementation Guide V24	Final	Production	●○○○○	No	$	No
Implementation Specification	NCPDP Telecommunication Standard, Implementation Guide, Version F2, March 2018 and Equivalent Batch Standard Implementation Guide, Version 15	Final	Pilot	●○○○○	No	$	No
Implementation Specification	NCPDP Batch Standard Medicaid Subrogation Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007	Final	Production	●●●●●	Yes	$	-
Emerging Implementation Specification	*NCPDP Batch Standard Medicaid Subrogation Implementation Guide, Version 10*	*Final*	*Pilot*	*Feedback Requested*	*No*	*$*	-

Limitations, Dependencies, and Preconditions for Consideration:

- The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link.
- The pharmacy telecommunication standard provides a standard format for the electronic submission of third party drug claims and other transactions between pharmacy providers, health plans (payers, insurance companies), third-party administrators, and others with financial responsibility.

Applicable Security Patterns for Consideration:

- All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

• Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), all covered entities – health plans, clearinghouses and covered health care providers are required to use the telecommunication standard for eligibility verification as well as claim and service billing, predetermination of benefits, and prior authorization. The standard can perform a variety of other functions as well. • Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated. • Costs to access the NCPDP standards is based on membership. NCPDP's Standards Matrix is available as a reference providing a high-level overview of the latest version/release and/or the most commonly used of NCPDP standards and implementation guides, as well as NCPDP's Data Dictionary and External Code List. • Additional information is available on testing, and the full cost on any of the X12 transactions. ASETT the HHS compliance tool to enable testing and complaint filing for all X12 and NCPDP transactions. • The Telecommunication Standard Implementation Guide Version F2 has been requested for adoption under HIPAA by NCVHS, and NCPDP is in the investigative stage of providing a test tool for this version. • For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set.	

Interoperability Need: Health Care Claim Status Request and Response

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	X12N/005010X212 Health Care Claim Status Request and Response (276/277), August 2006 as an ASC X12 Standards for Electronic Data Interchange Technical Report Type 3	Final	Production	●●●○○	Yes	$	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• The Administrative Simplification provisions of HIPAA apply to the adoption of electronic transaction standards and operating rules for use in the health care industry. HIPAA has some different requirements for information exchange than EHRs, but there is hope for convergence in the future. Information about the HIPAA regulations regarding standards and operating rules can be found at https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html. Readers can find information about requirements for covered entities and their business associates and enforcement from this link. • This standard and the transaction were adopted under the Health Insurance Portability Act of 1996 (HIPAA) to increase efficiency in the health care system by	• All covered entities and their business associates are required to comply with the HIPAA Privacy and Security Rules. Health and Human Services has partnered with the Office of the National Coordinator and the National Institutes of Standards and Technology to publish comprehensive guidance for Security specific to electronic protected health information. A self-assessment tool kit is available to support integrating privacy and security into practices.

reducing the use of paper and increasing the exchange of health care information electronically. This information is often maintained in provider practice management and billing systems but duplicates information in electronic health records. • Before implementation of a new version of a standard, end to end testing should be conducted with vendor systems and between trading partners to ensure changes have been accommodated. • Additional information is available on testing, and the full cost on any of the X12 transactions. • For a description of the functionality of each transaction, visit the X12 website. Click on a transaction set name to toggle the display of the purpose and scope of that transaction set.	

Operating Rules to Support Administrative Transactions

Interoperability Need: Operating Rules for Claims, Enrollment, and Premium Payments (Phase IV)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Operating Rules	CAQH CORE Phase IV Operating Rules Set	Final	Pilot	Feedback Requested	No	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- Operating rules were adopted as a requirement of the Patient Protection and Affordable Care Act of 2010, under section 1104, Administrative Simplification. Note: Phase IV operating rules have not yet been recommended for adoption by NCVHS but are available for *voluntary use*.
- Operating rules are intended to support and enhance the use of the standard transactions. They include additional requirements to help implement the transaction in a more uniform way across health plans, and ensure a more complete set of information in the response.
- Operating rules are developed through workgroups which are consensus driven, based on the members who participate. Greater participation from more diverse members will result in more robust content and utility to enable to the rules to support the transactions and serve the users effectively.
- The Phase IV CAQH CORE Operating Rules, available for use on a *voluntary basis* as of September 2015, include:
  - Phase IV CAQH CORE 450: Health Care Claim (837) Infrastructure Rule
  - Phase IV CAQH CORE 452: Health Care Services Review – Request for Review and Response (278) Infrastructure Rule
  - Phase IV CAQH CORE 454: Benefit Enrollment and Maintenance (834) Infrastructure Rule
  - Phase IV CAQH CORE 456: Payroll Deducted and Other Group Premium Payment for Insurance Products (820) Infrastructure Rule
  - Phase IV CAQH CORE 470: Connectivity Rule
- Testing or certification with the operating rules is voluntary and available through a vendor contracted to the authoring entity. The checklist is available on the website.
- CAQH CORE maintains a host of free implementation tools to support operating rule adoption on its website. Additionally, CAQH CORE offers regular educational webinars which are archived on its website to drive greater industry awareness of the value of operating rules in collaboration with leading healthcare organizations.

Applicable Security Patterns for Consideration:

Interoperability Need: Operating Rules for Electronic Funds Transfer (EFT) and Electronic Remittance Advice (ERA) for Payments and Reconciliation (Phase III)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	CAQH, Committee on Operating Rules for Information Exchange, Phase III CORE EFT & ERA Operating Rule Set Approved June 2012	Final	Production	●●●○○	Yes	Free	Yes[$]

Limitations, Dependencies, and Preconditions for Consideration:

- Operating rules were adopted as a requirement of the Patient Protection and Affordable Care Act of 2010, under section 1104, Administrative Simplification.
- Operating rules are intended to support and enhance the use of the standard transactions. They include additional requirements to help implement the transaction in a more uniform way across health plans, and ensure a more complete set of information in the response. For example, rather than just "yes or no" for eligibility information, the operating rule requires health plans to return patient eligibility and financial responsibility for a list of service types such as emergency care, inpatient hospitalization, and dental and vision services.
- Operating rules include other business rules to support the eligibility transaction as it moves between the provider and the health plan, such as the format of the health plan's companion guide (see CORE Rule 152), as well as response time for real time and batch transactions (see CORE Rules 155 and 156).
- Operating rules are developed through workgroups which are consensus driven, based on the members who participate. Greater participation from more diverse members will result in more robust content and utility to enable to the rules to support the transactions and serve the users effectively. This is where the convergence of administrative and clinical systems will take place with respect to patient benefit information in the electronic health record.
- These operating rules include CAQH CORE policies for voluntary testing and certification, which are not mandatory. The other rules support the EFT and ERA through a range of requirements, from the companion guide template, to the uniform use of combinations for certain Claim and Remark Codes (CARCs and RARCs), to certain standard data elements for enrolling providers electronically for EFT or ERA transactions.
- Phase III Operating Rules for Electronic Funds Transfer (EFT) and Electronic Remittance Advice (ERA) for Payments and Reconciliation include:
  - (1) Phase III CORE 350: Healthcare Claim Payment/Advice (835) Infrastructure Rule
  - (2) Phase III CORE 360: Uniform Use of CARCs and RARCs (835) Rule
  - (3) Phase III CORE 370: EFT and ERA Reassociation (CCD+/835) Rule
  - (4) Phase III CORE 380: EFT Enrollment Data Rule

Applicable Security Patterns for Consideration:

- Feedback requested.

▪ (5) Phase III CORE 382: ERA Enrollment Data Rule • Testing or certification with the operating rules is voluntary and available through a vendor contracted to the authoring entity. The checklist is available on the website. • CAQH CORE maintains a host of free implementation tools to support operating rule adoption on its website. Additionally, CAQH CORE offers regular educational webinars which are archived on its website to drive greater industry awareness of the value of operating rules in collaboration with leading healthcare organizations.	

Interoperability Need: Operating Rules to Support Electronic Prescribing Transactions

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	NCPDP Operating Rules for the X12 270/271 Transactions in Electronic Prescribing v1.0	Final	Production	Feedback Requested	No	$	No

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Feedback Requested	• Feedback requested.

Interoperability Need: Operating Rules to Support Eligibility and Claim Status Transactions (Phase II)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	CAQH, Committee on Operating Rules for Information Exchange, CORE Phase II Policies and Operating Rules, Approved July 2008, v5010, Update March 2011	Final	Production	●●●●○	Yes	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:	Applicable Security Patterns for Consideration:
• Operating rules were adopted as a requirement of the Patient Protection and Affordable Care Act of 2010, under section 1104, Administrative Simplification. • Operating rules are intended to support and enhance the use of the standard transactions. They include additional requirements to help implement the transaction in a more uniform way across health plans, and ensure a more complete set of information in the response. For example, rather than just "yes or no" for eligibility information, the operating rule requires health plans to return patient eligibility and financial responsibility for a list of service types such as emergency care, inpatient hospitalization, and dental and vision services. • Operating rules include other business rules to support the eligibility transaction as it moves between the provider and the health plan, such as the format of the health plan's companion guide (see CORE Rule 152), as well as response time for real time and batch transactions (see CORE Rules 155 and 156). • Operating rules are developed through workgroups which are consensus driven,	• Feedback requested.

based on the members who participate. Greater participation from more diverse members will result in more robust content and utility to enable to the rules to support the transactions and serve the users effectively. This is where the convergence of administrative and clinical systems will take place with respect to patient benefit information in the electronic health record.

- Phase II eligibility and claim status operating rules include:
  - (1) Phase II CORE 250: Claim Status Rule, version 2.1.0 March 2011 (Incorporated by reference in § 162.920).
  - (2) Phase II CORE 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule, version 2.1.0, March 2011. (Incorporated by reference in § 162.920).
  - (3) Phase II CORE 259: Eligibility and Benefits 270/271 AAA Error Code Reporting Rule, version 2.1.0. (Incorporated by reference in § 162.920).
  - (4) Phase II CORE 260: Eligibility & Benefits Data Content (270/271) Rule, version 2.1.0, March 2011. (Incorporated by reference in § 162.920).
  - (5) Phase II CORE 270: Connectivity Rule, version 2.2.0, March 2011. (Incorporated by reference in § 162.920).(b).
- Testing or certification with the operating rules is voluntary and available through a vendor contracted to the authoring entity. The checklist is available on the website.
- CAQH CORE maintains a host of free implementation tools to support operating rule adoption on its website. Additionally, CAQH CORE offers regular educational webinars which are archived on its website to drive greater industry awareness of the value of operating rules in collaboration with leading healthcare organizations.

Interoperability Need: Operating Rules to Support Eligibility Transactions (Phase I)

Type	Standard/Implementation Specification	Standards Process Maturity	Implementation Maturity	Adoption Level	Federally Required	Cost	Test Tool Availability
Implementation Specification	CAQH, Committee on Operating Rules for Information Exchange, CORE Phase I Policies and Operating Rules, Approved April 2006, v5010 Update March 2011	Final	Production	●●●●○	Yes	Free	Yes

Limitations, Dependencies, and Preconditions for Consideration:

- Operating rules were adopted as a requirement of the Patient Protection and Affordable Care Act of 2010, under section 1104, Administrative Simplification.
- Operating rules are intended to support and enhance the use of the standard transactions. They include additional requirements to help implement the transaction in a more uniform way across health plans, and ensure a more complete set of information in the response. For example, rather than just "yes or no" for eligibility information, the operating rule requires health plans to return patient eligibility and financial responsibility for a list of service types such as emergency care, inpatient hospitalization, and dental and vision services.

Applicable Security Patterns for Consideration:

- Feedback requested.

• Operating rules include other business rules to support the eligibility transaction as it moves between the provider and the health plan, such as the format of the health plan's companion guide (see CORE Rule 152), as well as response time for real time and batch transactions (see CORE Rules 155 and 156). • Operating rules are developed through workgroups which are consensus driven, based on the members who participate. Greater participation from more diverse members will result in more robust content and utility to enable to the rules to support the transactions and serve the users effectively. This is where the convergence of administrative and clinical systems will take place with respect to patient benefit information in the electronic health record. • Phase I eligibility operating rules include: ▪ (1) Phase I CORE 150: Batch Acknowledgement (not adopted) version 1.1.0, March 2011. (Incorporated by reference in § 162.920). ▪ (2) Phase I CORE 151 Real Time Acknowledgement (not adopted) version 1.1.0, March 2011. (Incorporated by reference in § 162.920). • Although Phase I CORE 150 & 151 operating rules are not part of the federal mandate for adoption of Phase I CAQH CORE Operating Rules, they are required for voluntary CORE Certification. ▪ (3) Phase I CORE 152: Eligibility and Benefit Real Time Companion Guide Rule, version 1.1.0, March 2011, and CORE v5010 Master Companion Guide Template. (Incorporated by reference in § 162.920). ▪ (4) Phase I CORE 153: Eligibility and Benefits Connectivity Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920). ▪ (5) Phase I CORE 154: Eligibility and Benefits 270/271 Data Content Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920). ▪ (6) Phase I CORE 155: Eligibility and Benefits Batch Response Time Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920). ▪ (7) Phase I CORE 156: Eligibility and Benefits Real Time Response Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920). ▪ (8) Phase I CORE 157: Eligibility and Benefits System Availability Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920). • Testing or certification with the operating rules is voluntary and available through a vendor contracted to the authoring entity. The checklist is available on the website. • CAQH CORE maintains a host of free implementation tools to support operating rule adoption on its website. Additionally, CAQH CORE offers regular educational webinars which are archived on its website to drive greater industry awareness of the value of operating rules in collaboration with leading healthcare organizations.	

Appendices

Appendices, including Sources for Security Standards/Security Patterns, Models and Profiles, Educational/Informational Resources, and State and Local Public Health Readiness for Interoperability are available for viewing online at www.healthit.gov/isa.