

**Table 2A – Adopted Content Exchange and Vocabulary Standards, ONC
Proposed Rule (pp. 79-81)**

Row #	Purpose	Category	Adopted Standard(s) to Support Meaningful Use Stage 1	Candidate Standard(s) to Support Meaningful Use Stage 2
<i>I</i>	<i>Patient Summary Record</i>	Cx	HL7 CDA R2 CCD Level 2 or ASTM CCR	Alternatives expected to be narrowed based on HIT Standards Committee recommendations
	•Problem List	V	Applicable HIPAA code set required by law (i.e., ICD-9-CM); or SNOMED CT®	Applicable HIPAA code set required by law (e.g., ICD-10-CM) or SNOMED CT®
	•Medication List	V	Any code set by an RxNorm drug data source provider that is identified by the United States National Library of Medicine as being a complete data set integrated within RxNorm+	RxNorm
	•Medication Allergy List	V	No standard adopted at this time.	UNII
	•Procedures	V	Applicable HIPAA code sets required by law (i.e., ICD-9-CM or CPT-4®)	Applicable HIPAA code sets required by law (i.e., ICD-10-PCS or CPT-4®)
	•Vital Signs	V	No standard adopted at this time.	CDA template
	•Units of Measure	V	No standard adopted at this time.	UCUM
	•Lab Orders and Results	V	LOINC® when LOINC® codes have been received from a laboratory	LOINC®

Row #	Purpose	Category	Adopted Standard(s) to Support Meaningful Use Stage 1	Candidate Standard(s) to Support Meaningful Use Stage 2
2	<i>Drug Formulary Check</i>	Cx	Applicable Part D standard required by law (i.e., NCPDP Formulary & Benefits Standard 1.0)	Applicable Part D standard required by law
3	<i>Electronic Prescribing</i>	Cx V	Applicable Part D standard required by law (e.g., NCPDP SCRIPT 8.1) or NCPDP SCRIPT 8.1 and NCPDP SCRIPT 10.6 Any code set by an RxNorm drug data source provider that is identified by the United States National Library of Medicine as being a complete data set integrated within RxNorm+	NCPDP SCRIPT 10.6 RxNorm
4	<i>Administrative Transactions</i>	Cx	Applicable HIPAA transaction standards required by law	Applicable HIPAA transaction standards required by law
5	<i>Quality Reporting</i>	Cx	CMS PQRI 2008 Registry XML Specification#,+	Potentially newer version(s) or standards based on HIT Standards Committee Input
6	<i>Submission of Lab Results to Public Health Agencies</i>	Cx	HL7 2.5.1	Potentially newer version(s) or standards based on HIT Standards Committee Recommendations
		V	LOINC® when LOINC® codes have been received from a laboratory	LOINC®, UCUM, and SNOMED CT® or Applicable Public Health Agency Requirements

Row #	Purpose	Category	Adopted Standard(s) to Support Meaningful Use Stage 1	Candidate Standard(s) to Support Meaningful Use Stage 2
7	<i>Submission to Public Health Agencies for Surveillance or Reporting (excluding adverse event reporting)</i>	Cx	HL7 2.3.1 or HL7 2.5.1	Potentially newer version(s) or standards based on HIT Standards Committee Input
		V	According to Applicable Public Health Agency Requirements	GIPSE or According to Applicable Public Health Agency Requirements
8	<i>Submission to Immunization Registries</i>	Cx	HL7 2.3.1 or HL7 2.5.1	Potentially newer version(s) or standards based on HIT Standards Committee Recommendations
		V	CVX*,+	CVX

Table 2B – Adopted Privacy and Security Standards from ONC Proposed Rule (p. 85)

Row #	Purpose	Adopted Standard
1	<i>General Encryption and Decryption of Electronic Health Information</i>	A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used (e.g., FIPS 197 Advanced Encryption Standard, (AES), Nov 2001).+
2	<i>Encryption and Decryption of Electronic Health Information for Exchange</i>	An encrypted and integrity protected link must be implemented (e.g., TLS, IPv6, IPv4 with IPsec). +
3	<i>Record Actions Related to Electronic Health Information (i.e., audit log)</i>	The date, time, patient identification (name or number), and user identification (name or number) must be recorded when electronic health information is created, modified, deleted, or printed. An indication of which action(s) occurred must also be recorded (e.g., modification).+
4	<i>Verification that Electronic Health Information has not been Altered in Transit</i>	A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit. The secure hash algorithm used must be SHA1 or higher (e.g., Federal Information Processing Standards (FIPS) Publication (PUB) Secure Hash Standard (SHS) FIPS PUB 180-3).+
5	<i>Cross-Enterprise Authentication</i>	Use of a cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (e.g., IHE Cross Enterprise User Assertion (XUA) with SAML identity assertions).+
6	<i>Record Treatment, Payment, and Health Care Operations Disclosures</i>	The date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure must be recorded.+