

of UCUM and SNOMED CT® for this exchange in the future would lead to improved interoperability.

vii. Submission to Public Health Agencies for Surveillance or Reporting

For the purposes of electronically submitting information to public health agencies for surveillance and reporting, Certified EHR Technology must be capable of using HL7 2.3.1 or HL7 2.5.1 as a content exchange standard. This requirement is not meant to include adverse event reporting. At this time, we have not adopted a specific vocabulary standard for submitting information to public health agencies for surveillance and reporting, and believe that such standards will be determined in large part by the applicable public health agency receiving such information. We look forward to receiving recommendations from the HIT Standards Committee regarding additional standards that should be adopted to facilitate the electronic

submission of information to public health agencies for surveillance and reporting purposes.

viii. Submission to Immunization Registries

For the purposes of electronically submitting information to immunization registries Certified EHR Technology must be capable of using HL7 2.3.1 or HL7 2.5.1 as a content exchange standard and the CDC maintained HL7 standard code set CVX—Vaccines Administered¹⁸ as the vocabulary standard.

ix. Table 2A

Table 2A below displays the applicable adopted standards for each exchange purpose specified. We have used “Cx” and “V” as shorthand for “content exchange” and “vocabulary,” respectively, to identify which standard category applies to the exchange purpose. Where a cell in table 2A includes the reference “no standard

adopted at this time” it means that a Complete EHR or EHR Module would not be required to be tested and certified as including a particular standard. As a result, any local or proprietary standard could be used as well as the standard(s) listed as candidate meaningful use Stage 2 standards. Unless marked with the following superscripts, all of the adopted standards are from the ONC process that took place prior to the enactment of the HITECH Act or are required by other HHS regulations.

- A number sign “#” indicates that the HIT Standards Committee recommended this standard to the National Coordinator but it was not part of the prior ONC process.

- An asterisk “*” indicates that the standard was neither recommended by the HIT Standards Committee nor part of the prior ONC process.

- A plus sign “+” as mentioned above indicates a standard that is not a voluntary consensus standard.

TABLE 2A—ADOPTED CONTENT EXCHANGE AND VOCABULARY STANDARDS

Row No.	Purpose	Category	Adopted standard(s) to support meaningful use stage 1	Candidate standard(s) to support meaningful use stage 2
1	Patient Summary Record	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®.
2	Drug Formulary Check	Cx	Applicable Part D standard required by law (i.e., NCPDP Formulary & Benefits Standard 1.0).	Applicable Part D standard required by law.
3	Electronic Prescribing	Cx	Applicable Part D standard required by law (e.g., NCPDP SCRIPT 8.1) or NCPDP SCRIPT 8.1 and NCPDP SCRIPT 10.6.	NCPDP SCRIPT 10.6.
		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.
4	Administrative Transactions	Cx	Applicable HIPAA transaction standards required by law.	Applicable HIPAA transaction standards required by law.
5	Quality Reporting	Cx	CMS PQRI 2008 Registry XML Specification ^{#,+} .	Potentially newer version(s) or standards based on HIT Standards Committee Input.

¹⁸ The CDC’s National Center of Immunization and Respiratory Diseases (NCIRD) maintains the

HL7 external code set CVX <http://www.cdc.gov/vaccines/programs/iis/stds/cvx.htm>.

TABLE 2A—ADOPTED CONTENT EXCHANGE AND VOCABULARY STANDARDS—Continued

Row No.	Purpose	Category	Adopted standard(s) to support meaningful use stage 1	Candidate standard(s) to support meaningful use stage 2
6	Submission of Lab Results to Public Health Agencies.	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.
7	Submission to Public Health Agencies for Surveillance or Reporting (excluding adverse event reporting).	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	Submission to Immunization Registries.	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.

c. Privacy and Security Standards

We believe it is necessary for Certified EHR Technology to provide certain privacy and security capabilities. In that regard, we have aligned adopted certification criteria to applicable HIPAA Security Rule requirements and believe that in doing so, such capabilities may assist eligible professionals and eligible hospitals to improve their overall approach to privacy and security. In addition, some may find that the capabilities provided by Certified EHR Technology may facilitate and streamline compliance with Federal and state privacy and security laws. We believe that the HIPAA Security Rule serves as an appropriate starting point for establishing the capabilities for Certified EHR Technology. That being said, the HITECH Act directs the HIT Policy Committee, the HIT Standards Committee, and ONC to look at capabilities beyond those explicitly specified in the HIPAA Security Rule. We intend to work with both of these Committees to explore these areas and where possible to adopt new certification criteria and standards in the future to improve the capabilities Certified EHR Technology can provide to protect health information.

The adopted certification criteria in Table 1 assure that Certified EHR Technology is capable of supporting eligible professionals and eligible hospitals comply with HIPAA requirements to protect electronic health information residing within Certified EHR Technology and, where appropriate, when such information is exchanged. For certain capabilities, we have adopted, after considering the recommendations of the HIT Standards Committee, specific standards to be used in Certified EHR Technology.

These standards and their purposes are displayed in Table 2B. For other capabilities, we have not adopted specific standards because such capabilities can be appropriately addressed through different approaches, and we did not want to preclude innovation. For example, while we have adopted a certification criterion related to access control, we have not adopted a specific standard for access control because we believe that the industry will continue to innovate at a rapid pace in this area and better methods to implement this capability will be available faster than we would be able to adopt them via regulation. On the other hand, we have adopted certification criteria and standards for encryption because specific industry best practices and requirements exist with respect to encryption and the strength of encryption algorithms. HHS previously articulated in guidance entitled “Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals” (74 FR 42741) that encryption is an effective method to “render protected health information unusable, unreadable, or indecipherable to unauthorized individuals,” and one that can exempt a HIPAA covered entity from having to report a breach. To further support this determination, we believe a logical and practical next step and one that will provide eligible professionals and eligible hospitals with a capability they may not have had in the past is to require Certified EHR Technology to be capable of encryption.

It is important to note, under 45 CFR 164.312(a)(2)(iv) and (e)(2)(ii), a HIPAA covered entity must assess whether encryption as a method for safeguarding

electronic protected health information is a reasonable and appropriate safeguard in its environment. Consequently, a HIPAA covered entity could be in compliance with the HIPAA Security Rule if it determines that encryption is not reasonable and appropriate in its environment and it documents its rationale and implements an equivalent alternative measure if reasonable and appropriate. We hope that by requiring Certified EHR Technology to include this capability, that the use of encryption will become more prevalent. Of the certification criteria and associated standards we have adopted related to encryption, the first is for encryption in general while the second is specific to when electronic health information is exchanged. The first certification criterion and standard will assure that Certified EHR Technology is capable of using encryption according to user-defined preferences. There are several industry best practices in this regard and we expect that with the availability of the capability to perform encryption, eligible professionals and hospitals will follow suit and enhance how they protect electronic health information. We anticipate that this capability could be used by eligible professionals and eligible hospitals to encrypt backup hard drives or tapes, removable media, or portable devices. Finally, we expect other functions or services such as domain name service, directory access, and consistent time (e.g., for audit logs) to support and further enable some of the standards in Table 2B. However, due to the fact these functions or services may be part of an overall implementation of Certified EHR Technology (e.g., operating system, network time server) rather than a specific capability Certified EHR

Technology should be tested and certified as including, we chose not to adopt certification criteria or standards. We request public comment on whether the previously mentioned functions or services or any other function or service should be considered for adoption by the Secretary as a necessary capability for Certified EHR Technology to include.

After considering the written and oral public comments provided to both the HIT Policy and HIT Standards Committees, we would like to clarify the applicability of the privacy and security certification criteria and standards adopted in this interim final rule. This interim final rule strictly focuses on the

capabilities of Certified EHR Technology and does not change existing HIPAA Privacy Rule or Security Rule requirements, guarantee compliance with those requirements, or absolve an eligible professional, eligible hospital, or other health care provider who adopts Certified EHR Technology from having to comply with any applicable provision of the HIPAA Privacy or Security Rules. While the capabilities provided by Certified EHR Technology may assist an eligible professional or eligible hospital in improving their technical safeguards in order to meet some or all of the HIPAA Security Rule's requirements or influence their risk analysis, the use of

Certified EHR Technology alone does not equate to compliance with the HIPAA Privacy or Security Rules. The capabilities provided by Certified EHR Technology do not affect in any way the analysis a HIPAA covered entity is responsible for performing specified at 45 CFR 164.306(b) and (d). Unless there are specific meaningful use measures for privacy and security that require the use of a particular capability, an eligible professional or eligible hospital may find that its security practices exceed these capabilities and nothing in this rule precludes the use or implementation of more protective privacy and security measures.

TABLE 2B—ADOPTED PRIVACY AND SECURITY STANDARDS

Row No.	Purpose	Adopted standard
1	General Encryption and Decryption of Electronic Health Information.	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	Encryption and Decryption of Electronic Health Information for Exchange.	An encrypted and integrity protected link must be implemented (e.g., TLS, IPv6, IPv4 with IPsec). ⁺
3	Record Actions Related to Electronic Health Information (i.e., audit log).	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	Verification that Electronic Health Information has not been Altered in Transit.	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 SHA-1 or higher (e.g., Federal Information Processing Standards (FIPS) Publication (PUB) Secure Hash Standard (SHS) FIPS PUB 180-3). ⁺
5	Cross-Enterprise Authentication	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	Record Treatment, Payment, and Health Care Operations Disclosures.	The date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure must be recorded. ⁺

3. Adopted Implementation Specifications

Pursuant to section 3004 of the PHSA, the Secretary is required to adopt implementation specifications in addition to standards and certification criteria. Implementation specifications, which for HIPAA covered transaction standards are found in implementation guides, provide specific configuration instructions and constraints for implementing a particular standard or set of standards. Because some standards can be implemented in several different ways, these specifications are critical in some cases to make interoperability a reality—simply using a standard does not necessarily guarantee interoperability.

Standards Development Organizations (SDOs), HITSP, and others have developed implementation specifications with varying degrees of specificity, which in turn have resulted in varying degrees of interoperability. In some cases, the standards used in the

NHIN, for example, have been constrained even further and resulted in a narrow and unique set of implementation specifications, designed for a specific architecture and well-defined exchange. Based on input from HIT Standards Committee, we understand that very few implementation specifications are widely used and most are immature or too architecturally specific for adoption by large segments of the HIT industry before meaningful use Stage 2.

Given the importance of implementation specifications and the analyses and field testing necessary to refine them, we do not believe, with the exception of the few mentioned below, that there are mature implementation specifications ready to adopt to support meaningful use Stage 1. We seek public comment on whether there are in fact implementation specifications that are industry-tested and would not present a significant burden if they were adopted. We believe that certain exchange

purposes such as electronic prescribing and laboratory test results, already have available some of the most mature implementation specifications. We will consider adopting implementation specifications, though, for any or all adopted standards provided that there is convincing evidence submitted in public comment of the specifications' maturity and widespread usage.

We have adopted a certification criterion requiring that Certified EHR Technology be capable of using the standard, CMS PQRI 2008 Registry XML Specification, for quality reporting. We have also adopted as the implementation specifications for this standard, the Physician Quality Reporting Initiative Measure Specifications Manual for Claims and Registry. Additionally, as we noted above we have adopted standards that require Certified EHR Technology to be capable of using applicable HIPAA transaction standards adopted by HHS for eligibility for health plan