the Common Clinical Data Set may be beneficial for other purposes, including participation in HHS payment programs. We request comment on whether we should adopt a separate 2015 Edition health IT certification criterion for the voluntary testing and certification of health IT to the capability to create a summary record formatted to the C-CDA Release 2.0 with or without the ability to meet the requirements of the Common Clinical Data Set definition.

C-CDA Data Provenance Request for Comment

As the exchange of health data increases, so does the demand to track the provenance of this data over time and with each exchange instance. Confidence in the authenticity, trustworthiness, and reliability of the data being shared is fundamental to robust privacy, safety, and security enhanced health information exchange. The term "provenance" in the context of health IT refers to evidence and attributes describing the origin of electronic health information as it is captured in a health system and subsequently persisted in a way that supports its lifespan. As described in the President's Council of Advisors on Science and Technology (PCAST) Report "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans"[88], provenance includes information about the data's source and the processing that the data has undergone. The report refers to "tagged data elements" as units of data accompanied by a "metadata tag" that describes the attributes, provenance, and required security protections of the data.

In April 2014, ONC launched the Data Provenance Initiative within the Standards and Interoperability (S&I) Framework to identify the standards necessary to capture and exchange

[88] PCAST Report to the President: Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf

provenance data, including provenance at time of creation, modification, and time of exchange.[89] The stakeholder community represented a wide variety of organizations including health IT developers; federal, state, and local agencies; healthcare professionals; research organizations; payers; labs; and individuals within academia. In the fall of 2014, the HL7 IG for CDA Release 2: Data Provenance, Release 1 (US Realm) (DSTU)[90] was published. This IG clarifies existing content from various standards within HL7[91] and describes how provenance information for a CDA document in a health IT system should be applied, and what vocabulary should be used for the metadata. This includes provenance metadata in the CDA at the header, section and entry levels. We seek comment on the maturity and appropriateness of this IG for the tagging of health information with provenance metadata in connection with the C-CDA. Additionally, we seek comment on the usefulness of this IG in connection with certification criteria, such as ToC and VDT certification criteria.

- Clinical Information Reconciliation and Incorporation

2015 Edition Health IT Certification Criterion
§ 170.315(b)(2) (Clinical information reconciliation and incorporation)

We propose to adopt a 2015 Edition "clinical information reconciliation and incorporation" certification criterion that is a revised (but largely similar to the 2014 Edition Release 2) version of the "clinical information reconciliation and incorporation" criterion adopted at § 170.314(b)(9).

Incorporation System Performance

---

[89] http://wiki.siframework.org/Data+Provenance+Initiative

[90] http://wiki.hl7.org/index.php?title=HL7_Data_Provenance_Project_Space and http://gforge.hl7.org/gf/project/cbcc/frs/?action=FrsReleaseBrowse&frs_package_id=240

[91] Standards including HL7 Clinical Documentation Architecture Release 2 (CDA R2), HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, and HL7 Version 2 Vocabulary & Terminology Standards (all are normative standards)

criterion. This trust bundle specification's focuses on "guidance on the packaging and distribution of Trust Bundles to facilitate scalable trust between Security/Trust Agents (STAs)." As we understand, including this specification as part of certification could enable patient-facing technology to be configured to trust externally hosted bundles of S/MIME certificates. In addition, we have continued to hear concerns regarding the difficulties related to exchanging Direct messages across platforms and "trust communities" in the context of patient-directed transmissions. Therefore, we also request comments on whether any additional requirements are needed to support scalable trust between STAs as well as ways in which ONC, in collaboration with other industry stakeholders, could support or help coordinate a way to bridge any gaps.

C-CDA Creation Capability Request for Comment

We request public comment on a potential means to provide explicit implementation clarity and consistency as well as to further limit potential burdens on health IT developers. Specifically, should we limit the scope of C-CDA creation capability within this certification criterion to focus solely on the creation of a CCD document template based on the C-CDA Release 2.0? This approach could also have the benefit of creating clear expectations and predictability for other health IT developers who would then know the specific document template implemented for compliance with this criterion.

C-CDA Data Provenance Request for Comment

We refer readers to the request for comment under the same heading ("C-CDA Data Provenance Request for Comment") in the ToC certification criterion earlier in this section of the preamble (section III). The request for comment focuses on the maturity of the HL7 IG for CDA

Release 2: Data Provenance, Release 1 (US Realm) (DSTU) [151] and its potential use in connection with the C-CDA.

- Clinical Summary

We note that we are not proposing a 2015 Edition "clinical summary" certification criterion because past versions of this certification criterion were adopted in direct support of the EHR Incentive Programs. The proposals found in the EHR Incentive Programs Stage 3 proposed rule published elsewhere in this issue of the **Federal Register** rely on patients being provided with the ability to view, download, and transmit their health information via online access. Therefore, we believe the capabilities included in the 2015 Edition "view, download, and transmit to 3rd party" certification criterion appropriately and sufficiently support the proposals of the EHR Incentive Programs.

- Secure Messaging

2015 Edition Health IT Certification Criterion
§ 170.315(e)(2) (Secure messaging)

We propose to adopt a 2015 Edition "secure messaging" certification criterion that is unchanged in comparison to the 2014 Edition "secure messaging" criterion (§ 170.314(e)(3)).

- Transmission to Immunization Registries

2015 Edition Health IT Certification Criterion
§ 170.315(f)(1) (Transmission to immunization registries)

We propose to adopt a 2015 Edition "transmission to immunization registries" certification criterion that is revised in comparison to the 2014 Edition "transmission to immunization registries" criterion (§ 170.314(f)(2)). We propose to adopt an updated IG, require

[151] http://wiki.hl7.org/index.php?title=HL7_Data_Provenance_Project_Space and http://gforge.hl7.org/gf/project/cbcc/frs/?action=FrsReleaseBrowse&frs_package_id=240

We propose to adopt a 2015 Edition "authentication, access control, and authorization" certification criterion that is unchanged in comparison to the 2014 Edition "authentication, access control, and authorization" criterion (§ 170.314(d)(1)).

- Auditable Events and Tamper-Resistance

2015 Edition Health IT Certification Criterion
§ 170.315(d)(2) (Auditable events and tamper-resistance)

We propose to adopt a 2015 Edition "auditable events and tamper-resistance" certification criterion that is unchanged in comparison to the 2014 Edition "auditable events and tamper-resistance" criterion (§ 170.314(d)(2)). We seek comment, however, on two issues. In August 2014, the HHS Office of Inspector General (OIG) released a report entitled "The Office of the National Coordinator for Health Information Technology's Oversight of the Testing and Certification of Electronic Health Records."[134] In that report, the OIG found that ONC approved test procedures did not address common security issues, including "logging emergency access or user privilege changes." The OIG therefore recommended "…that ONC work with NIST to strengthen EHR test procedure requirements so that the ATCBs [ONC-Authorized Testing and Certification Bodies] can ensure that EHR vendors incorporate common security and privacy features into the development of EHRs."[135]

The standards adopted at § 170.210(e) and referenced by the 2014 Edition "auditable events and tamper-resistance" and "audit report(s)" certification criteria require that technology must be able to record audit log information as specified in sections 7.2 through 7.4, 7.6 and 7.7 of the standard adopted at 45 CFR 170.210(h). The standard adopted at § 170.210(h) is ASTM

[134] http://oig.hhs.gov/oas/reports/region6/61100063.pdf
[135] http://oig.hhs.gov/oas/reports/region6/61100063.pdf

E2147.[136] Section 7.6 of ASTM E2147 specifies that audit log content needs to include the "type of action" and references six "actions:" additions, deletions, change, queries, print, and copy. Section 7.7 requires that the audit log record when patient data is accessed. So while not explicitly referenced in section 7.6, the action of "access" or viewing of a patient's information is also required to be recorded for certification. Moreover, we clarify that an "emergency access" event is expected to be recorded (just like any other access) in accordance with section 7.7.

Because it does not appear that the ASTM standard indicates recording an event when an individual's user privileges are changed, we seek comment on whether we need to explicitly modify/add to the overall auditing standard adopted at 170.210(e) to require such information to be audited or if this type of event is already audited at the point of authentication (e.g., when a user switches to a role with increased privileges and authenticates themselves to the system). We also seek comments on any recommended standards to be used in order to record those additional data elements.

In a 2013 report entitled "Not All Recommended Safeguards Have Been Implemented in Hospital EHR Technology (OEI-01-11-00570),"[137] the OIG recommended that ONC should propose a revision to this certification criterion to require that EHR technology keep the audit log operational whenever the EHR technology is available for updates or viewing or, alternatively, CMS could update its meaningful use criteria to require providers to keep the audit log operational whenever EHR technology is available for updates or viewing.[138] As a result of that report, in the Voluntary Edition proposed rule, we proposed an "auditable events and tamper resistance" certification criterion that would have required technology to prevent all users from

---

[136] http://www.astm.org/Standards/E2147.htm. The standard is also incorporated by reference at 45 CFR 170.299(c)(1) and available at the Office of the Federal Register.
[137] https://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf
[138] https://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

being able to disable an audit log. While several commenters supported the proposal, an equal share expressed concern, including the HITSC. The HITSC recommended against implementing this proposal, indicating that the requirements of the 2014 Edition certification criterion (identifying only a limited set of users that could disable the audit log and logging when and by whom an audit log was disabled and enabled) provided sufficient parameters to determine the accountable party in the event of a security incident. [139] Other commenters contended that including an absolute prohibition would be problematic because there are valid and important reasons for users to disable the audit log, including allowing a system administrator to disable the audit log for performance fixes, stability, disaster recovery, and system updates or allowing a system administrator to disable it when there is rapid server space loss which is hindering a provider from accessing needed clinical information in a timely manner.

We reiterate our policy first espoused with the adoption of the 2014 Edition "auditable events and tamper resistance" certification criterion in that the ability to disable the audit log must be restricted to a limited set of users to meet this criterion. The purpose of this certification criterion is to require health IT to demonstrate through testing and certification that it has certain security capabilities built in. As we have evaluated both OIG's input and that of commenters, we believe our certification criterion is appropriately framed within the parameters of what our regulation can reasonably impose as a condition of certification. This regulation applies to health IT and not to the people who use it. Thus, how an individual provider or entity chooses to ultimately implement health IT that has been certified to this or any other certification criterion does so outside the scope of this regulation.

---

[139] http://www.healthit.gov/FACAS/sites/faca/files/Baker_PSWG_2015editionnprm_public_comment_V2.pdf

We also received feedback to the Voluntary Edition proposed rule that there may be some events recorded in the audit log that may be more critical to record than other events. Commenters noted that there may be a critical subset of events that should remain enabled at all times, while other events could be turned off during critical times or for system updates by a subset of users. As noted above, the standards adopted at § 170.210(e) and referenced by the 2014 Edition "auditable events and tamper-resistance" certification criterion requires that health IT technology must be able to record additions, deletions, changes, queries, print, copy, access. The 2014 Edition also required the log to record when the audit log is disabled and by whom and that such capability must be restricted to a limited set of identified users. As a result, we again seek comment on whether:

- there is any alternative approach that we could or should consider;
- there is a critical subset of those auditable events that we should require remain enabled at all times, and if so, additional information regarding which events should be considered critical and why; and
- Any negative consequences may arise from keeping a subset of audit log functionality enabled at all times.

- Audit Report(s)

2015 Edition Health IT Certification Criterion
§ 170.315(d)(3) (Audit report(s))

We propose to adopt a 2015 Edition "audit reports(s)" certification criterion that is unchanged in comparison to the 2014 Edition "audit reports(s)" criterion (§ 170.314(d)(3)).

- Amendments

2015 Edition Health IT Certification Criterion
§ 170.315(d)(4) (Amendments)

(iii) Data. (A) TIN;

(B) NPI;

(C) Provider type;

(D) Patient insurance;

(E) Patient age;

(F) Patient sex in accordance with, at a minimum, the version of the standard specified in § 170.207(n)(1);

(G) Patient race and ethnicity in accordance with, at a minimum, the version of the standard specified in § 170.207(f)(2);

(H) Patient problem list data in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4); and

(I) Practice site address.

(d) Privacy and security--(1) Authentication, access control, and authorization. (i) Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed; and

(ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

(2) Auditable events and tamper-resistance--(i) Record actions. Technology must be able to:

(A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1);

(B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and

(C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by technology in accordance with the standard specified in § 170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section).

(ii) Default setting. Technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraph (d)(2)(i)(B) or (C) of this section, or both paragraphs (d)(2)(i)(B) and (C).

(iii) When disabling the audit log is permitted. For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of users.

(iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the technology.

(v) Detection. Technology must be able to detect whether the audit log has been altered.

(3) Audit report(s). Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards in § 170.210(e).

(4) Amendments. Enable a user to select the record affected by a patient's request for amendment and perform the capabilities specified in paragraph (d)(4)(i) or (ii) of this section.

(i) Accepted amendment. For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location.

(ii) Denied amendment. For a denied amendment, at a minimum, append the request and denial of the request to the affected record or include a link that indicates this information's location.

(5) Automatic access time-out. (i) Automatically stop user access to health information after a predetermined period of inactivity.

4. We propose that a user would need to be able to be able to configure the technology to set the time period within which data would be used to create the export summary or summaries. And that this must include the ability to enter in a start and end date range as well as the ability to set a date at least three years into the past from the current date.
5. We propose that a user would need to be able to configure the technology to create an export summary or summaries based on the following user selected events:
    - A relative date or time (e.g., the first of every month);
    - A specific date or time (e.g., on 10/24/2015); and
    - When a user signs a note or an order.
6. We propose that a user would need to able to configure and set the storage location to which the export summary or export summaries are intended to be saved.

Again, we emphasize that all these capabilities would need to be able to be configured and executed by a user without the aid of additional health IT developer personnel and without the need to request developer action. Further, we also reiterate that we have expanded the nature and focus of this criterion to more precisely address provided critiques as well as to expand the anticipated and potential uses providers can deploy based on this more configuration focused criterion.

- Data Segmentation for Privacy

We propose to adopt two new certification criteria that would focus on the capability to separately track ("segment") individually identifiable health information that is protected by rules that are more privacy-restrictive than the HIPAA Privacy Rule. This type of health information is sometimes referred to as sensitive health information. The HIPAA Privacy Rule

serves as the federal baseline for health information privacy protections. It also generally permits the use or disclosure of protected health information (PHI) for limited specific purposes (such as treatment and payment) without a patient's permission.[108]

The HIPAA Privacy Rule does not override (or preempt) more privacy-protective federal and state privacy laws. A number of federal and state health information privacy laws and regulations are more privacy-protective than the HIPAA Privacy Rule. Typically, these rules require a patient's permission (often referred to as "consent" in these rules) in writing in order for the individually identifiable health information regulated by those laws to be shared. One example is the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (42 CFR part 2) ("part 2") that apply to information about treatment for substance abuse from federally funded programs.[109] There are also federal laws protecting certain types of health information coming from covered U.S. Department of Veterans Affairs facilities and programs (38 U.S.C. 7332). These laws and comparable state laws were established, in part, to address the social stigma associated with certain medical conditions by encouraging people to get treatment and providing them a higher degree of control over how their health information may be shared. These laws place certain responsibilities on providers to maintain the confidentiality of such information. More restrictive state laws also protect certain categories of individually identifiable health information, such as information regarding minors or teenagers, intimate partner/sexual violence, genetic information, and HIV-related information.[110] These laws and regulations remain in effect and changes to these laws and regulations are not within the scope of this

---

[108] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/
[109] http://www.healthit.gov/sites/default/files/privacy-security/gwu-data-segmentation-final-cover-letter.pdf.
[110] http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy.

proposed rule.[111] However, with these laws in mind, the proposals that follow seek to encourage the development and use of a technical capability that permits users to comply with these existing laws and regulations. These proposals are also in line with the Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap Version 1.0.[112] HHS is committed to encouraging the development and use of policy and technology to advance patients' rights to access, to amend, and to make choices for the disclosure of their electronic individually identifiable health information. HHS also noted support for the development of standards and technology to facilitate patients' ability to control the disclosure of specific information that is considered by many to be sensitive in nature (such as information related to substance abuse treatment, reproductive health, mental health, or HIV) in an electronic environment.[113]

Technological advances are creating opportunities to share data and allow patient preferences to electronically persist in health IT. In 2012, ONC launched the Data Segmentation for Privacy (DS4P) initiative through ONC's Standards and Interoperability (S&I) Framework. [114] The DS4P initiative aimed to provide technical solutions and pilot implementations to help meet existing legal requirements in an increasingly electronic environment. [115] The DS4P initiative worked to enable the implementation and management of varying disclosure policies in an electronic health information environment in an interoperable manner. Overall, the DS4P initiative and its subsequent pilots focused on the exchange of health information in the context of 42 CFR part 2 and sought to develop technical standards that would enable a provider to adopt

---

[111] For a policy discussion, see Substance Abuse and Mental Health Services Administration (SAMHSA)'s recent public listening session pertaining to the federal confidentiality of regulations: https://www.federalregister.gov/articles/2014/05/12/2014-10913/confidentiality-of-alcohol-and-drug-abuse-patient-records.

[112] http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf

[113] http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf

[114] http://wiki.siframework.org/Data+Segmentation+for+Privacy+Use+Cases

[115] For more information about enabling privacy through data segmentation technology, see http://www.healthit.gov/providers-professionals/enabling-privacy

health IT that could segment electronic sensitive health information regulated by more restrictive laws and make compliance with laws like Part 2 more efficient. Since the sunset of the DS4P initiative in April 2014, there have been live implementations and public testimony regarding the success and practical application of the DS4P standard. Organizations including the Substance Abuse and Mental Health Services Administration (SAMHSA), the U.S. Department of Veterans Affairs (VA), and private companies that participated in the initiative have moved to production use of DS4P. For example, a stakeholder who implemented the DS4P part 2 solution noted that the DS4P technical capability implemented in parts of Florida has saved some hospitals millions of dollars associated with the cost of care because the patients they treat with substance use issues or behavioral health issues were able to send an electronic referral and get a discharge performed earlier in the process.[116] Another technology stakeholder incorporated the DS4P technical functionality into its behavioral health and general hospital health IT solutions released this year. Most recently, SAMHSA developed an open source technology for patient consent management that uses the DS4P standard.[117] In September 2014, this technical solution was deployed into a live environment at a public health department.

The technical specifications are outlined in the HL7 Version 3 Implementation Guide: DS4P, Release 1 (DS4P IG), Part 1: CDA R2 and Privacy Metadata.[118] The DS4P IG describes the technical means of applying security labels (privacy metadata) which can be used to enact any security or privacy law, regulation, or policy so that the appropriate access control decisions

---

[116] See Health IT Policy Committee's (HITPC) Privacy and Security Tiger Team Public Meeting, Transcript, (Apr. 16, 2014), p. 14, http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-04-16.pdf

[117] http://www.healthit.gov/providers-professionals/ds4p-initiative

[118] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=354 . Completed Normative Ballot in January 2014 and was successfully reconciled in February 2014. HL7 approved the final standard for publication and ANSI approved in May 2014.

will be made regarding downstream use, access or disclosure for specially protected data so that appropriate metadata tags are applied.

Conceptually, the DS4P approach utilizes metadata applied in layers (e.g. metadata applied to the header, section, or entry levels of a C-CDA document). The DS4P technical approach defaults to privacy metadata tagging at the document level. If an organization chooses to apply additional privacy metadata tagging within a document, that optional technical capability is also described within the IG for CDA. If a receiving system is unable to process section or entry level privacy metadata, the default is tagging at the document level. The approach relies on certain electronic actions being taken by both the sending system and the receiving system. The sending system must:

1. Identify information that requires enhanced protection or is subject to further restrictions;
2. Verify that the patient's privacy consent decision allows for the disclosure of health information;[119] and
3. Add privacy metadata to the health information being disclosed.

In turn, the receiving system must:

1. Be able to process the privacy metadata associated with the received health information; and
2. Verify the patient's consent before re-disclosure, if the receiving system has a need to re-disclose the information.

Data segmentation technology emerged to enable health care providers' use of technology to comply with existing privacy laws, regulations, and policies. The term "data

[119] http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange

segmentation" is often used to describe the electronic labeling or tagging of a patient's health information in a way that allows patients or providers to electronically share parts,[120] but not all, of a patient record. For example, data segmentation technology can be applied to the sharing of electronic sensitive health information, because that information is afforded greater protections under various state and federal laws,[121] as is discussed above. In this proposed rule, we propose to offer two certification criteria that would allow for health IT to be presented for testing and certification to the DS4P standard. We view the proposed offering of certification to these criteria as an initial step on technical standards towards the ability of an interoperable health care system to compute and persist the applicable permitted access, use or disclosure; whether regulated by state or federal laws regarding sensitive health information or by an individual's documented choices about downstream access to, or use or disclosure to others of, the identifiable individual's health information. The application of the DS4P standard at the document level is an initial step. We understand and acknowledge additional challenges surrounding the prevalence of unstructured data, sensitive images, and potential issues around use of sensitive health information by CDS systems. The adoption of document level data segmentation for structured documents will not solve these issues, but will help move technology in the direction where these issues can be addressed.

For example, today, electronic sensitive health information is not typically kept in the same repository as non-sensitive data. If security labels were applied to C-CDA documents at the time they are created (see "data segmentation for privacy – send" certification criterion), the receiving system would have more choices about how to store and use that sensitive information.

---

[120] The HL7 approved standard does allow for tagging at the data element level, but this proposed rule is suggesting just applying the DS4P to the document level.

[121] http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy

If the receiving system had the capability to grant access to the tagged documents by using the security labels as part of the access control decision, then co-mingling the tagged, sensitive health information with the non-sensitive data becomes more achievable.

In July 2014, the HITPC provided recommendations on the use of DS4P technology to enable the electronic implementation and management of disclosure policies that originate from the patient, the law, or an organization, in an interoperable manner, so that electronic sensitive health information may be appropriately shared.[122] The HITPC noted a clear need to provide coordinated care for individuals with mental health and/or behavioral health issues. The HITPC recognized that the ability of patients to withhold consent to disclose information remains a concern for providers. In particular, providers want to provide the best care for patients, but they have concerns about incomplete records due to both professional obligation and liability considerations. While the need for providers to act on incomplete information is not necessarily new, the use of health IT may create an expectation of more complete information.[123] In recognition of the consumer, business, clinical, and technical complexities, the HITPC suggested a framework of two glide paths for the exchange of 42 CFR part 2-protected data, based on whether the subject is sending or receiving information. [124] As a first step in the glide path, the HITPC recommended that we include Level 1 (document level tagging) send and receive functionality. [125] Document level is the most basic level of privacy metadata tagging described in

---

[122] See Health IT Policy Committee (HITPC) Recommendation Letter to ONC, July 2014, http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf; see also HITPC's Privacy and Security Tiger Team Public Meeting, Transcript, May 12, 2014, http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-05-12.pdf; Public Meeting, Transcript, May 27, 2014, http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-05-27.pdf.

[123] Id.

[124] For more details on the two glide paths for part 2-protected data, see http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf.

[125] Id. See also, related HITPC recommendations pertaining to data segmentation submitted to ONC in September 2010: http://www.healthit.gov/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf.

the DS4P standard. The following two proposals would implement the HITPC's recommendations.

- Data Segmentation for Privacy – Send

2015 Edition Health IT Certification Criterion
§ 170.315(b)(7) (Data segmentation for privacy – send)

A provider currently cannot send sensitive patient information electronically without some technical capability to indicate information is subject to restrictions, such as a prohibition on re-disclosure without consent, consistent with 42 CFR part 2. The sending provider also must have confidence that the receiver can properly handle electronically sent 42 CFR part 2-covered data. Because neither of these functionalities are currently supported in certification, sensitive health information such as 42 CFR part 2-covered data is often only shared via paper and fax. We propose, consistent with the HITPC recommendations, that for certification to this criterion, a Health IT Module must be able to send documents using document level tagging (Level 1) in accordance with the DS4P IG. Document level tagging enables health IT to send the 42 CFR part 2-covered data along with the appropriate privacy metadata tagging and keep it sequestered from other data. The DS4P IG, which includes Level 1 functionality, provides guidance to allow, with proper authorization, a system to send a C-CDA with tags indicating any restrictions (such as a prohibition on re-disclosure without consent). While the DS4P IG specifies the technical means for applying privacy metadata tagging to C-CDA documents, it also optionally supports use of privacy metadata tagging within the document (at the section and entry levels). We only propose to require the document level functionality for sending as part of certification to this criterion.

- Data Segmentation for Privacy – Receive

2015 Edition Health IT Certification Criterion
§ 170.315(b)(8) (Data segmentation for privacy – receive)

In general, 42 CFR part 2-covered data is not currently provided electronically to healthcare providers through electronic exchange. Instead, the status quo remains to share 42 CFR part 2-covered data via paper and fax. In line with the HITPC recommendations, we propose a certification criterion that would require a Health IT Module to be able to receive 42 CFR part 2-covered data in accordance with the DS4P IG. DS4P at the document level (Level 1) of the recommendations allows recipient health IT to receive, recognize, and view documents with privacy metadata tagging indicating certain restrictions from 42 CFR part 2 providers with the document sequestered from other health IT data. A recipient provider could use document level tagging to sequester the document from other documents received and help prevent unauthorized re-disclosure, while allowing the sensitive data to flow more freely to authorized recipients. Thus, consistent with the HITPC recommendations, we propose that a Health IT Module be able to receive documents tagged with privacy metadata tagging (Level 1).

- Care Plan

2015 Edition Health IT Certification Criterion
§ 170.315(b)(9) (Care plan)

We propose to adopt a new 2015 Edition certification criterion that would reflect a Health IT Module's ability to enable a user to record, change, access, create and receive care plan information in accordance with the "Care Plan document template" in the C-CDA Release 2.0 standard.

The S&I Framework Longitudinal Coordination of Care (LCC) Longitudinal Care Plan Sub-Work Group defined a "care plan" as "the synthesis and reconciliation of the multiple plans of care produced by each provider to address specific health concerns. It serves as the blueprint shared by all participants to guide the individual's care. As such, it provides the structure

include the ability to enter in a start and end date range as well as the ability to set a date at least three years into the past from the current date.

(iv) Event configuration. A user must be able to configure the technology to create an export summary or summaries based on the following user selected events:

(A) A relative date or time (e.g., the first of every month);

(B) A specific date or time (e.g., on 10/24/2015); and

(C) When a user signs a note or an order.

(v) Location configuration. A user must be able to configure and set the storage location to which the export summary or export summaries are intended to be saved.

(7) Data segmentation for privacy – send. Technology must enable a user to create a summary record formatted in accordance with each of the standards adopted in § 170.205(a)(3) and (4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1).

(8) Data segmentation for privacy – receive. Technology must enable a user to:

(i) Receive a summary record that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1);

(ii) Apply document-level tagging and sequester the document from other documents received; and

(iii) View the restricted document (or data), without incorporating the document (or data).

(9) Care plan. Technology must enable a user to record, change, access, create, and receive care plan information in accordance with the Care Plan document template in the standard adopted in § 170.205(a)(4).

seeking testing and certification to (h)(4) for interoperability purposes. As part of this proposed certification criterion, we propose that directory sources must demonstrate the capability to respond to provider directory queries according to the IHE HPD profile. Additionally, as part of the certification criteria, we propose that the directory sources must respond to the following provider directory queries

- Query for an individual provider;
- Query for an organizational provider; and
- Query for relationships between individual providers and organizational providers.

In addition we propose including an optional capability within this certification criterion to address federated requirements. In this optional capability, we propose that the Health IT Module would be required to follow the approved federation option of for IHE HPD to accomplish querying in federated environments. The federation change proposal was approved in September, 2014 was incorporated into the IHE HPD Profile.

- Electronic Submission of Medical Documentation

2015 Edition Health IT Certification Criterion
§ 170.315(i)(1) (Electronic submission of medical documentation)

We propose to adopt a new certification criterion as part of the proposed 2015 Edition at § 170.315(i)(1) that would focus on the electronic submission of medical documentation.

According to CMS, the Medicare Fee for Service (FFS) program currently spends in excess of $360 billion annually to provide services to over 35 million beneficiaries (excludes Medicare eligible individuals enrolled in non-FFS Medicare Programs).[198] The 2013 CMS Office

[198] http://www.hhs.gov/budget/fy2015/fy-2015-budget-in-brief.pdf

of Financial Management (OFM) Improper Payment Report[199] noted that 12.7% (or $45.8 B) of the payments from the Medicare trust fund were for claims for services that were either: 1) not medically necessary and appropriate based on documentation that was submitted; or 2) insufficiently documented to determine if the billed service was necessary.

To respond to Congress' mandate[200] to more effectively manage improper payments, while recognizing the importance of reducing administrative burden for providers, CMS OFM's Provider Compliance Group (PCG) established the electronic submission of Medical Documentation (esMD) program to begin to enable the electronic submission of medical documentation.[201] As part of this program, CMS worked with ONC to establish the "esMD Initiative" under the S&I Framework.[202] This initiative created use cases and identified appropriate standards to facilitate the electronic exchange of medical documentation among providers and Medicare FFS review contractors. Currently, esMD Phase 1 supports the submission of unstructured data in PDF format. This method of submission is broadly deployed and accounts for over 25% of all Medicare FFS post-payment medical review submissions. In addition to post-payment review, new demonstration programs are focused on prior-authorization for specific services that have high improper payment rates. Prior-authorization ensures appropriate documentation is reviewed prior to these services/items being performed or delivered in order to avoid post-payment denials that may affect the beneficiary, the provider, or both.

---

[199] http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/CERT/index.html?redirect=/cert
[200] http://www.whitehouse.gov/sites/default/files/omb/financial/_improper/PL_107-300.pdf; http://www.gpo.gov/fdsys/pkg/PLAW-112publ248/pdf/PLAW-112publ248.pdf; and www.whitehouse.gov/sites/default/files/omb/financial/_improper/PL_111-204.pdf
[201] http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/index.html?redirect=/ESMD
[202] http://wiki.siframework.org/esMD+-+Charter+and+Members

In addition to current methods for submitting medical documentation (e.g., mail, fax, PDF), Medicare FFS seeks to also enable a standardized and interoperable electronic approach that would reduce the time, expense, and paper required in current manual processes used for prior authorization, pre-payment review, post-payment audit, and quality management. Acceptable methods must ensure that providers are able to submit any documentation they believe is required in order to show that a proposed or provided service meets applicable requirements.

The esMD Initiative electronic Determination of Coverage (eDoC) workgroup provided an open forum for providers and payers to establish a mutual understanding of the requirements necessary for submission of structured medical documentation to support prior authorization, pre-payment review and post-payment audit. Standards analysis by the workgroup revealed a significant gap in the current standards with respect to uses that went beyond the exchange of a summary care record between providers. To address this gap, participants in the eDoC workgroup created a new Clinical Documents for Payers – Set 1 (CDP1) IG to further extend and constrain the C-CDA Release 2.0 standard.

Non-repudiation of signatures for electronic submission of medical documentation was a complementary challenge faced by the esMD Initiative. While keeping in mind the cost and impact of certain requirements, the esMD Initiative focused on two approaches to digital signatures. The “Author of Record Level 1” use case addressed the need for digital signatures on groups of documents and on single transactions. The “Author of Record Level 2” use case focused on digital signatures that could be embedded in HL7 CDA documents and included support for multiple signers where each declares their role and signature purpose. In addition to the ability to support digital signatures using industry standards, the use cases also addressed a

standards-based method for the delegation, by a holder of a digital certificate, of the right to sign on their behalf by another holder of a digital certificate. While digital signatures have been implemented in the healthcare industry for other purposes, this effort will extend their use to declare and secure the provenance of single documents, bundles of documents, and transactions. The use of digital signatures on C-CDA documents will guarantee the identity of the author and ensure the integrity of the data once the document has been signed.

In summary, the esMD Initiative and its participants successfully produced standards and implementation guides to help minimize improper payments; improve interoperability for electronic submission of medical documentation, including parameters for non-repudiation, and reduce administrative burden associated with prior authorization, pre-payment review, post-payment audit and quality management.

In light of this work, we propose to adopt a certification criterion at § 170.315(i)(1) to support the electronic submission of medical documentation that includes four specific capabilities, which are each discussed in more detail below. As we mentioned in the Executive Summary of this proposed rule and discuss in more detail under section IV.B of this preamble (Modifications to the ONC Health IT Certification Program), we propose to broaden the scope of the ONC Health IT Certification Program beyond just focusing on supporting the EHR Incentive Programs. As such, we seek to make clear that this certification criterion is not within those programs' scope and is meant to be available to support other CMS program policy objectives as well as health care providers' ability to communicate encounter documentation to a payer, in particular to satisfy Medicare FFS coverage determination rules.

Capability 1 – We propose that a Health IT Module be able to support the creation of a document in accordance with the HL7 Implementation Guide for CDA Release 2: Additional

CDA R2 Templates – Clinical Documents for Payers – Set 1, Release 1 – US Realm[203] in combination with the C-CDA Release 2.0 standard (proposed for adoption at § 170.205(a)(4)). We propose to adopt the most recent version of the CDP1 IG at § 170.205(a)(5)(i).[204] The CDP1 IG is designed to be used in conjunction with C-CDA Release 2.0 templates and makes it possible for providers to exchange a more comprehensive set of clinical information. For example, payers such as Medicare FFS allow providers to submit any information they believe substantiates that a service is medically necessary and appropriate under the applicable coverage determination rules.

A Health IT Module's support for the document-level templates formatted in accordance with the CDP1 IG would ensure that the technology is able to communicate all information relative to a patient encounter or assert that information for each "required" section is not available/included. If the provider then applies a digital signature to the document (as discussed in more detail below), the result is a non-repudiation declaration of the encounter information.

The CDP1 IG was balloted in February of 2014 and should complete balloting this spring.[205] The February 2014 balloted version includes the following new templates:

1) Five (5) new or additionally constrained document level templates:

- Enhanced Encounter Document
- Enhanced Hospitalization Document
- Enhanced Operative Note Document
- Enhanced Procedure Document

---

[203] http://www.hl7.org/special/Committees/claims/index.cfm. We also note that access to the current draft of the CDP1 IG is freely available for review during the public comment period by establishing an HL7 user account.
[204] This would be the version of the IG (DSTU) that completes the ballot cycle before issuance of a subsequent final rule.
[205] http://www.hl7.org/special/Committees/claims/index.cfm. We also note that access to the current draft of the CDP1 IG is freely available for review during the public comment period by establishing an HL7 user account.

- Interval Document

2) Four (4) new section level templates:
    - Additional Documentation Section
    - Externally Defined Clinical Data Elements Section
    - Placed Orders Section
    - Transportation Section
3) Three (3) additionally constrained C-CDA Release 2.0 section level templates:
    - Functional Status Section
    - Plan of Treatment Section
    - Social History Section
4) New or additionally constrained entry level templates that provide support for new section level templates.

The most recent changes to the CDP1 IG include:

- Expanded descriptions regarding the use of the IG;
- References to and a list of additional constraints for templates that are based on the C-CDA Release 2.0 templates;
- Updates required for conformance with the published version of the C-CDA Release 2.0 ;
- Removal of attestation language and addition of a document succession description (clarification of standard C-CDA document succession);
- Technical corrections; and
- Name changes for the IG and the individual document level templates.

The CDP1 IG enables documentation to be completely and accurately conveyed in the new document templates. To do this, the document level templates referenced by the CDP1 IG require the inclusion of the referenced section level templates, which also include additional specificity and constraints. While a Health IT Module would need to support the entry of additional information, providers would not necessarily be required to collect any additional information to satisfy the new constraints. In other words, a specific nullFlavor may be used by the Health IT Module when creating the CDP1 IG document to indicate that no information is available for the relevant section or entry level template. Likewise, the Health IT Module may enable the provider to indicate that while information is present in the medical record it is not applicable to the purpose for which the document is intended and would subsequently result in an appropriate nullFlavor in the created CDP1 document.

To meet this capability included in the proposed certification criterion, a Health IT Module must be able to create a document that also conforms to the CDP1 IG's requirements along with appropriate use of nullFlavors to indicate when information is not available in the medical record for section or entry level template required in the CDP1 IG. In addition, a conformant Health IT Module must also demonstrate the ability to generate the document level templates as defined in the C-CDA Release 2.0, including the unstructured document.

We propose to further refine this certification criterion's scope relative to the applicable document templates within the C-CDA Release 2.0 and CDP1 IG that would need to be tested and certified for specific settings for which a Health IT Module is designed. Specifically, we propose that a Health IT Module:

- Would, regardless of the setting for which its designed, need to be tested and certified to the following document templates:

- Diagnostic Imaging Report;
- Unstructured Document;
- Enhanced Operative Note Document;
- Enhanced Procedure Note Document; and
- Interval Document.

- Designed for the ambulatory setting would also need to be certified to the Enhanced Encounter Document.
- Designed for the inpatient setting would also need to be certified to Enhanced Hospitalization Document.

Capability 2 – We propose that a Health IT Module be able to support the use of digital signatures embedded in C-CDA Release 2.0 and CDP1 IG documents templates by adopting the HL7 Implementation Guide for CDA Release 2: Digital Signatures and Delegation of Rights, Release 1 (DSDR IG) (proposed for adoption at § 170.205(a)(5)(ii)).[206] This DSDR IG defines a method to embed digital signatures in a CDA document and provides an optional method to specify delegation of right assertions that may be included with the digital signatures. We note, however, that for the purposes of certification, we propose to require that that optional method must be demonstrated to meet this certification criterion. The implementation of this IG will allow payers, such as Medicare, to accurately authenticate the authorized signers of CDA document and trust the validity and authenticity of signed medical documentation. The DSDR IG provides specific guidance on the use of digital signatures embedded in a CDA document to:

- Provide a non-repudiation signature that attests to the role and signature purpose of each authorized signer to the document.

[206] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=375

- Provide for a delegation of rights where the signer is a delegated signer and not the authorized signer responsible individual or organization (e.g., the signer is acting as an authorized agent).
- Define the method of incorporating multiple digital signatures and delegation of right assertions into the header of a CDA document.
- Define how to create the digest of the CDA document
- Define how to sign and incorporate the:
    - CDA digest;
    - Timestamp;
    - Role of the signer;
    - Purpose of signature.
- Define how to incorporate the:
    - The public certificate of the signer;
    - Long term validation data, including Online Certificate Status Protocol (OCSP) response and/or Certificate Revocation List (CRL).

Digital signatures ensure that the recipient of the signed document can authenticate the authorized signer's digital certificate, the signature artifact(s), determine the signer's role and signature purpose and validate the data integrity of the document. To create a valid digital signature that meets Federal Information Processing Standards (FIPS)[207], Federal Information Security Management Act of 2002 (FISMA)[208], and Federal Bridge Certification Authority

[207] http://www.nist.gov/itl/fips.cfm
[208] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

(FBCA) requirements[209], the system used to digitally sign C-CDA Release 2.0 or CDP1 IG documents in accordance with the DSDR IG must meet the following requirements:

1) The cryptographic module[210] used must:
    a. Be validated to meet or exceed FIPS 140-2, Level 1.
    b. Implement a digital signature system and hash function must be compliant with FIPS 186-2 and FIPS 180-2.
    c. Store the private key on a FIPS 140-2 Level 1 validated cryptographic module using a FIPS-approved encryption algorithm.
2) The system must support multi-factor authentication that meets or exceeds Level 3 assurance as defined in NIST SP 800-63-2.
3) The system must set a 10-minute inactivity time period after which the certificate holder must re-authenticate the password to access the private key.
4) For software implementations, when the signing module is deactivated, the system must clear the plain text private key from the system memory to prevent the unauthorized access to, or use of, the private key.
5) The system must have a time system that is synced with the official National Institute of Standards and Technology time source (as described by the standard adopted at 45 CFR 170.210(g)).

For the purposes of testing and certification, we propose that the first requirement (cryptographic module requirements) be met through compliance documentation. For all other

---

[209] http://www.idmanagement.gov/sites/default/files/documents/FBCA%20Certificate%20Policy%20v2.27.pdf

[210] A cryptographic module is defined in FIPS 140-2 as "a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary."

specific capabilities in the list above, we expect testing and certification to assess the capabilities expressed.

We also propose that a Health IT Module must demonstrate the ability to validate a digital signature embedded in a C-CDA Release 2.0 document that is conformant with the DSDR IG. The requirements to perform this action are included in the DSDR IG.

Capability 3 – We propose that a Health IT Module be able to support the creation and transmission of "external digital signatures" for documents. These digital signatures may be used to sign any document for the purpose of both data integrity and non-repudiation. The esMD Initiative defines the requirements in the Author of Record Level 1: Implementation Guide.[211] We propose to adopt this IG at § 170.205(a)(5)(iii). The Author of Record Level I IG uses the IHE DSG standard to provide a signer with the ability to digitally sign multiple documents and embed the W3C compliant XADES signature in a signature document that may accompany the signed documents or as a "wrapper" for the documents. This signing capability is intended for use when the sender of one or more documents needs to ensure that the transmitted documents include the non-repudiation identity of the sender and ensure that the recipient can validate that the document s have not been altered from the time of signing. This is not intended to replace the ability to embed multiple digital signatures in a C-CDA Release 2.0 and CDP1 IG document. The Author of Record Level 1 IG provides specific guidance on the use of a single digital signature, external to document, to:

- Provide a non-repudiation signature that attests to the identity of the signer;
- Allows the recipient to validate the data integrity of the signed document;

---

211 http://wiki.siframework.org/file/view/esMD%20AoR%20Level%201%20Implementation%20Guide%20v5%20FINAL.docx/539084894/esMD%20AoR%20Level%201%20Implementation%20Guide%20v5%20FINAL.docx

- Provide for a delegation of rights where the signer is a delegated signer and not the authorized signer responsible individual or organization (e.g., the signer is acting as an authorized agent); and
- Defines how to incorporate the public certificate of the signer.

Digital signatures ensure that the recipient of the signed document can authenticate the authorized signer's digital certificate, the signature artifact(s), and validate the data integrity of the document. The system requirements in place to apply digital signatures on documents are the same as in capability 2 with the addition of a requirement that specifies that a Health IT Module must be able to digitally sign single or bundles of documents in conformance with the Author of Record Level 1 IG.

Capability 4 – We propose that a Health IT Module be able to support the creation and transmission of digital signatures for electronic transactions for the purpose of both data integrity and non-repudiation authenticity. The esMD Initiative defines the requirements in the Provider Profiles Authentication: Registration Implementation Guide.[212] We propose to adopt this IG at § 170.205(a)(5)(iv). The Provider Profiles Authentication: Registration IG uses the W3C XADES digital signature standard to "sign" the contents of an electronic transaction and include the signature as accompanying metadata in the signed transaction. This signing capability is intended for use when the sender or recipient of a transaction needs to ensure that the transmitted information include the non-repudiation identity of the sender and ensure that the recipient can validate that the authenticity and integrity of the transaction information. This is not intended to replace the digital signature requirements defined in either Capability 2 or 3 above. The Provider

---

212 http://wiki.siframework.org/file/view/esMD%20Use%20Case%201%20Implementation%20Guide%20V24%20FINAL.docx/539084920/esMD%20Use%20Case%201%20Implementation%20Guide%20V24%20FINAL.docx

Profiles Authentication: Registration IG provides specific guidance on the creation and use of a single digital signature for an electronic transaction, as accompanying metadata, to:

- Provide a non-repudiation signature that attests to the identity of the signer;
- Allow the recipient to validate the data integrity of the signed transaction;
- Provide for a delegation of rights where the signer is a delegated signer and not the authorized signer responsible individual or organization (e.g., the signer is acting as an authorized agent); and
- Define how to incorporate the public certificate of the signer.

Digital signatures ensure that the recipient of the signed transaction can authenticate the authorized signer's digital certificate, the signature artifact(s), and validate the data integrity of the transaction. The system requirements in place to apply digital signatures for transactions are the same as in capability 2 with the addition of a requirement that specifies that a Health IT Module must be able to digitally sign a transaction and create the appropriate metadata in conformance with the Provider Profiles Authentication: Registration IG.

4. Gap Certification Eligibility Table for 2015 Edition Health IT Certification Criteria

We define gap certification at 45 CFR 170.502 as the certification of a previously certified Complete EHR or EHR Module(s) to: (1) all applicable new and/or revised certification criteria adopted by the Secretary at subpart C of part 170 based on the test results of a NVLAP-accredited testing laboratory; and (2) all other applicable certification criteria adopted by the Secretary at subpart C of part 170 based on the test results used to previously certify the Complete EHR or EHR Module(s) (for further explanation, see 76 FR 1307-1308). Our gap certification policy focuses on the differences between certification criteria that are adopted through rulemaking at different points in time. This allows health IT to be certified to only the