eHealth Exchange

Operating Policy and Procedure

Subject: Safeguarding Controlled Unclassified Information (CUI)		
Status: FINAL – Approved by CC	**Policy #: OPP-13**	
Effective Date: 8/1/2020	**Version: 5.0**	**Page 1 of 5**

I. Purpose

The purpose of this Operating Policy and Procedure is to clarify non-Federal Participant obligations are to safeguard Controlled Unclassified Information (CUI) and to establish the CUI Performance and Service Specifications.

II. Background

Executive Order 13556 and 32 CFR Part 2002 require Federal Participants to protect Controlled Unclassified Information (CUI) and establish contractual obligations to safeguard CUI when they share CUI with nonfederal organizations.[1] The regulations direct Federal Participants to include in contracts with organizations that are not federal agencies a requirement that the non-federal agency that receives CUI comply with certain information security standards to safeguard CUI. The Coordinating Committee has worked closely with the Federal Participants to develop an approach that satisfies the legal requirements of the CUI Program without creating an undue burden on non-Federal Participants.

The regulations further direct Federal Participants to mark any information that is CUI Specified according to CUI Registry listed markings, unless it is impractical for the agency to individually mark CUI due to the nature or quantity of the information, or when an agency has issued a limited CUI marking waiver. Presently, there is no standardized practice or content standard to specify how to electronically tag CUI Specified with respect to Message Content. However, HL7® is currently working through a proposal to identify a value set for CUI Specified labels, which would also include markings indicating confidentiality level protection, handling instructions required by applicable policy, etc. Once HL7® establishes CUI codes, which will promote interoperability across HL7® Version 2, CDA, and FHIR® content, the Coordinating Committee will review the codes to develop implementing policies and procedures.

NIST developed Special Publication 800-171 Revision 1 ("Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations") and 800-171A ("Assessing Security Requirements for CUI") to assist the private sector in complying with the CUI Program. The NIST 800-171, Revision 1 states that, "[t]he security requirements apply to all components of nonfederal systems and organizations that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations."

The Coordinating Committee has adopted NIST Special Publications 800-171 Revision 1 as the CUI Performance and Service Specifications for the eHealth Exchange. The

[1] 32 C.F.R. § 2002.16

DURSA requires any eHealth Exchange Participant that receives CUI to comply with the CUI Performance and Service Specifications. This Operating Policy and Procedure provides additional guidance for eHealth Exchange Participants that are not federal government agencies but that receive CUI.

The CUI Performance and Service Specifications adopt NIST Special Publication 800-171 Revision 1 and apply to any non-Federal Participant that receives CUI from a Federal Participant. Non-Federal Participants are already required by the DURSA to comply with HIPAA as a base standard to protect the privacy and security of Protected Health Information (PHI). The HIPAA Security Rule requires covered entities and business associates to implement physical, administrative and technical safeguards to protect the security, confidentiality and integrity of PHI.

There are some differences between the HIPAA Security Rule and the requirements in NIST Special Publications 800-171 Revision 1. NIST Special Publication 800-171 Revision 1 requires recipients of CUI to develop a System Security Plan that describes system boundaries, system environments of operation, as well as how security requirements are implemented, and the relationships with or connections to other systems. Among other provisions, it also requires recipients of CUI to develop Plans of Action, which are designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems, and to describe how and when any unimplemented security requirements will be met. Each non-Federal Participant that receives CUI will need to address, in its Plans of Action, how the Participant will comply with those aspects of NIST Special Publication 800-171 Revision 1 that they do not currently address.

NIST Special Publication 800-171A, “Assessing Security Requirements for Controlled Unclassified Information,” provides a methodology and procedures to determine if security safeguards are implemented correctly, operating as intended, and satisfy CUI requirements.

Neither the NIST Special Publications nor the eHealth Exchange Performance and Service Specifications prescribe any particular approach to how a Participant prepares its System Security Plan. Indeed, NIST Special Publication 800-171 Revision 1 states that “Nonfederal organizations can implement a variety of potential security solutions either directly or using managed services, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement.” *See* NIST Special Publication 800-171 Revision 1, Ch. 3, pg. 8.

III. Policy

A. The Performance and Service Specifications include:

1. NIST Special Publication 800-171 Revision 1

B. Any non-Federal eHealth Exchange Participant that receives CUI shall comply with the CUI Performance and Service Specifications.

IV. Procedure

In order for eHealth Exchange to comply with the requirements of the Federal Participants regarding the CUI Program, the following steps need to be taken:

1. Participants shall review all CUI requirements identified in NIST Special Publication 800-171 Revision 1.
2. The Coordinating Committee will work with Non-Federal Participants to evaluate the above requirements and assess the burden to determine the impacts to Non-Federal Participants.
3. The Coordinating Committee will establish a Technical Task Group to leverage HL7 Security Workgroup efforts around labeling to specifically identify the standards that specify how and where both C-CDA and/or native documents are marked as well as define any necessary meta-tags. This OPP will be updated to include any new standards and/or technical specifications as recommended by the Workgroup.
4. The Coordinating Committee shall adopt standards and /or technical specifications, including any HL7 CUI codes, recommended by its technical Task Group regarding how electronic documents should be marked and how recipients should handle CUI. It is anticipated the Coordinating Committee will adopt these standards and/or technical specifications by 01/01/2020 which corresponds with this OPP's Effective Date. If the Coordinating Committee has not adopted these standards and/or technical specifications as of 01/01/20, then the Coordinating Committee may amend this OPP to take effect on the date on which the Coordinating Committee adopts these standards and/or technical specifications."
5. eHealth Exchange Staff will monitor NIST for future officially published revisions to NIST 800-171 revisions to notify the Coordinating Committee that adopting new revisions should be considered for adoption by this OPP.
6. Non-Federal Participants shall develop a system security plan and identify and address any gaps in compliance with the CUI Performance and Service

Specifications. Within twenty-four (24) months from the effective date of this OPP, Non-Federal Participants shall comply with the CUI Performance and Service Specifications.

V. Definitions

Controlled Unclassified Information: (CUI) is information the Federal Government creates or possesses, or that an entity creates or possesses for or on behalf of the Federal Government, that a law, regulation, or Federal Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information[2] or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

DURSA: Shall mean "Restatement II of the Data Use and Reciprocal Support Agreement (DURSA)," Version Date: September 30, 2014 or Restatement III of the DURSA if Restatement III has been formally adopted before the Effective Date of this OPP.

NIST: Shall mean the National Institute of Standards and Technology
All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the DURSA.

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the DURSA.

[2] *Classified information* is information that Executive Order 13526, "Classified National Security Information," December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, requires agencies to mark with classified markings and protect against unauthorized disclosure.

VI. References

1. Executive Order 13556-Controlled Unclassified Information, 3 CFR 13556, Nov. 4, 2010
2. 32 CFR Part 2002, Controlled Unclassified Information
3. "Restatement II of the Data Use and Reciprocal Support Agreement (DURSA)", Version Date: August 13, 2019
    a. Section 14.02, Business Associate Agreement
4. NIST Special Publication 800-171, Revision 1
5. NIST Special Publication 800-171A

VII. Version History

	Date	Comments
1	5/30/2019	Original Approved Version
2	8/13/2019	Modified the effective date to 01/01/2020 from 09/01/2019, reinforced that the Coordinating Committee can change effective dates when necessary, required eHealth Exchange staff to monitor NIST for future officially published revisions to NIST 800-171 revisions, required eHealth Exchange staff to notify the Coordinating Committee when new revisions are finalized so the Coordinating Committee can consider revising this OPP to adopt the new revision, and removed the informational crosswalk table that may have caused confusion.
3	6/2020	Updated language to reflect newest DURSA amendment changes; Updated formatting for consistency and readability