



OP&P 13 - Safeguarding Controlled Unclassified Information (CUI)

June 7, 2019 - All Participant Web Meeting

Controlled Unclassified Information (CUI) Background

- Presidential Executive Order 13556 (November 4, 2010)
- Intended to create uniform security policies and practices across federal government regarding confidential information not classified under the national security framework
- **Mandatory** participation by federal agencies
- Federal agencies must include in contracts with organizations that are not federal agencies a requirement to safeguard CUI
- The CUI Program is administered by NARA which maintains the CUI Registry, the common library of “markings” to be applied to CUI
- NARA commissioned NIST to develop a standard for the types of security controls that must be used by non –federal agencies that retain CUI, the result is [NIST 800-171](#) (revision 1)

OP&P 13 - Safeguarding Controlled Unclassified Information (CUI)

1. Participants' security teams should identify any gaps they have with NIST 800-171:

NIST SP 800-171 controls	NIST 800-53 Security Controls	Corresponding HIPAA Security Rule 45 C.F.R.	CUI
3.1.8	AC-7	Critical	Required for CUI
3.1.9	AC-8	Low	Required for CUI
3.1.10	AC-11	Critical	Required for CUI
	AC-11(1)		Required for CUI
3.1.22	AC-22		Required for CUI
	IR-7		Required for CUI
3.8.4	MP-3	Low	Required for CUI
3.8.8	MP-7(1)		Required for CUI
3.10.6	PE-17		Required for CUI
	RA-5(5)		Required for CUI
3.12.2	CA-5	High	Required for CUI
3.13.3	SC-2		Required for CUI
3.13.4	SC-4		Required for CUI
3.13.9	SC-10		Required for CUI
3.13.10	SC-12		Required for CUI
3.13.12	SC-15		Required if data is stored in the Cloud
3.13.14	SC-19		Required if VOIP is used
3.13.15	SC-23	Critical	Required for CUI

OP&P 13 - Safeguarding Controlled Unclassified Information (CUI)

2. Based upon Participants' current state of NIST 800-171 compliance, the Coordinating Committee will assess the burden of full compliance.
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.
4. This OPP will be updated to include any new standards and/or technical specifications as recommended by the Workgroup.
5. Non-Federal Participants shall develop a system security plan and identify and address any gaps in compliance with the CUI Performance and Service Specifications.
6. Within twenty-four (24) months from the effective date of this OPP, Non-Federal Participants shall comply with the CUI Performance and Service Specifications.

OP&P 13 - Safeguarding Controlled Unclassified Information (CUI)

7. Effective Date:

- This OP&P will not be effective until the Coordinating Committee adopts [standards and/or technical specifications](#), including any [HL7 CUI codes](#), recommended by its technical Task Group regarding how clinical 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 09/01/2019 which is why that date has been listed as the Effective Date for this OPP.
- If the Coordinating Committee has not adopted these standards and/or technical specifications as of 09/01/19, then the Effective Date of this OP&P will be delayed to the date on which the Coordinating Committee adopts these standards and/or technical specifications