CENTERS FOR MEDICARE & MEDICAID SERVICES
Office of Information Technology (OIT)
7500 Security Boulevard
Baltimore, Maryland 21244

CMS Chief Information Officer (CIO) Policy Framework

Issued:	09/15/2015
Last Revised:	05/24/2023
Document Control #:	CMS-CIO-POL-1000.04

Record of Changes

Version	Date	Author/Owner	Description of Change
1.0	09/15/2015	OEI/DPPIG	Baseline version of policy.
1.01	12/21/2015	OEI/DPPIG	Minor errors corrected.

2.0	12/14/2017	OIT/ICPG/DIIMP	• Routine policy review. Changes made to reflect OIT organizational structure.
			• Document review requirements changed from annual to three-year review cycle.
			• The CIO Policy Vetting and Clearance Process was updated to reflect the following:
			  ○ Combined Levels I and II reviews (OIT Group Director Review was combined with the CMS Critical Partners Review for expediency).
			  ○ Removed specific process steps from the Vetting and Clearance section and moved them to a standard operating procedure to allow for greater flexibility in improving the process without having to change the policy.
			• Changes to role of Policy Owner (see page 9)
			• Removed the role of the CTO (subsumed in the role of the Policy Owner).

3.0	08/28/2018	OIT/ICPG/DIIMP	• Update CMS Deputy CIO in roles and responsibilities • Update TRB in roles and responsibilities • Minor errors corrected.
4.0	05/24/2013	OIT/ICPG/DIIMP	Updated CIO Policy Vetting and Clearance Process to allow more flexibility to the review process. Replaced CIO Policy Officer with DIIMP to align with broader policy support within the division Moved information from the Appendices into the policy to minimize duplication and improve flow of overall policy process.

Effective Date / Approval

This policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it and remains in effect until it is rescinded, modified or superseded by another policy.

This policy must not be implemented in any recognized bargaining unit until the union has been provided notice of the proposed changes and given an opportunity to fully exercise its representational rights.

Signature: /s/
George Hoffmann
Deputy Chief Information Officer
Deputy Director (Policy), Office of Information Technology

Policy Owner's Review Certification

This document must be reviewed in accordance with the established review schedule located on the CMS website.

Signature: /s/

Cora Tracy
Director, IT Capital Planning Group
Office of Information Technology

Table of Contents

1 Policy Statement

The Centers for Medicare & Medicaid Services (CMS) Chief Information Officer (CIO) Policy Framework governs the development, review, approval, maintenance, and revocation of agency-level CIO policy documents written by CMS or on behalf of CMS. CIO policy documents include policies, technical standards, directives, guidelines, and procedures that encompass topics related to information technology (IT) and information security and privacy.

This policy serves to:

- Establish standards for the development and clearance of CIO policies
- Establish CIO policy standards of content, uniform format, and style
- Establish requirements for maintaining the administrative records documenting the development and issuance of all CIO policies
- Require periodic reviews of existing CIO policies to determine the need for revision and/or improvement
- Describe the revocation process for applicable CIO policies

The CMS CIO Policy Framework also formally establishes the *CIO Policy Vetting and Clearance Process* for CIO policy review and approval. *See Appendix 1: CIO Policy Life Cycle.*

Finally, this framework specifies:

- A structure and criteria for what should be categorized as a CIO policy, guideline, directive, technical standard, or procedure
- Processes for CIO Policy Framework life cycle activities
- Ongoing roles and responsibilities associated with CIO policy development and maintenance

This CIO policy is being revised in accordance with the review requirements specified in this document. This issuance supersedes the former policy *CMS CIO Policy Framework*, numbered CMS-CIO-POL-1000.02 and dated 09/25/2018.

2 Background

An important foundational element in support of the CMS IT governance program involves establishing an agency-level CIO policy function. The CIO policy function resides with the Office of Information Technology (OIT) with delegated responsibilities for policy development, coordination, education, and maintenance. The responsibilities associated with the CMS CIO Policy Framework include:

- Coordination of CIO policy and underlying development, dissemination, education, and maintenance

- Review and analysis of existing CIO policies for continued applicability and effectiveness
- Interpretation of current policy related to specific issues, situations and incidents

CIO policies articulate CMS' vision, strategy, and core values as they relate to the management and use of information and information technology resources, while supporting CMS' mission - *as an effective steward of public funds, CMS is committed to strengthening and modernizing the nation's health care system to provide access to high quality care and improved health at lower cost.*

Further, CIO policies ensure compliance with applicable laws and regulations and with all other authoritative sources such as mandates, directives, executive orders, and HHS policy. Finally, CIO policies help to promote operational efficiency and manage risk to the agency by specifying requirements and standards for the consistent management of IT resources across CMS.

3 Scope

All facets of CIO policy development, review, maintenance, and revocation, as stated in this policy, are in effect and apply to all agency-level CIO policies. It is important to note that IT policies and related documents developed specifically for the operations of individual Centers, Offices, Groups, or Divisions (i.e., developed for a limited audience) are out of scope.

This policy applies to all CMS employees and organizations conducting business for and on behalf of CMS through contractual relationships when managing and using CMS IT resources. This policy does not supersede any other applicable law or higher-level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

4 CIO Policy Documentation Hierarchy at CMS

The CMS CIO Policy Framework uses agency-level policies, directives, guidelines, procedures, and technical standards to convey IT Governance.

Categories of CIO documents are described below.

4.1 Policy

A policy is a guiding principle, direction, or expectation typically established by CMS senior management to influence and determine decisions. A CIO Policy is usually predicated on oversight requirements. Typical characteristics: (1) Includes clear, concise and simple language and complies with the Plain Language Act of 2010; (2) Contains "must" statements; (3) Addresses what the rule is rather than how to implement it; (4) Is readily available to all affected parties; (5) Results in punitive actions for failure to comply.

CMS CIO policies are mandatory. All new or substantially revised CIO policies require agency-wide vetting and clearance by the CIO. Once complete, these policies are submitted for version control and posted on the public-facing CMS website. *Note: Policies containing sensitive information are subject to restricted distribution and may not be posted on the CMS website.*

Approved by: CIO

Applicability: CMS-wide; all CMS employees, researchers and organizations conducting business for and on behalf of CMS through contractual relationships

Examples of CIO Policies:

- Policy for Information Technology (IT) Investment Management & Governance
- Policy for Section 508 Compliance

Purpose	Other Characteristics
• Have broad application throughout CMS • Articulates CMS' vision, strategy, and core values as they relate to the management and use of information and CIO resources • Guides CMS' decisions and directs individual behavior • Supports and enhances CMS 'mission • Clarifies requirements and exceptions • Ensures compliance with applicable laws and regulations • Helps manage risk to the Agency • Helps promote operational efficiency and consistency	• Independent of specific technologies • Short, concise, clear • Must be implementable and enforceable • Accountability for implementation must be specified • Includes definition of terms (that are consistent across policies) • Links to templates and other related guidance

4.2 CIO Directive

A CIO Directive allows the CIO to respond to identified gaps in CMS policy and instruction. Directives are used to issue direction on policy-level issues where current direction does not exist. CIO Directives may also serve as a stop-gap to provide immediate guidance while a policy is being developed/updated, cleared, and approved. CIO Directives may require action or may be for informational purposes to help clarify existing policy.

Approved by: CIO

Applicability: CMS-wide; all CMS employees, researchers and organizations conducting business for and on behalf of CMS through contractual relationships when using CMS CIO resources.

Examples of CIO Directives:

- CIO Library Guidance Hub

4.3 CMS Technical Standards

For the purposes of this policy, a technical standard refers to one or more related technical specifications that have been internally developed, sanctioned, and mandated for use by CMS. CMS' technical standards are documented in the form of the CMS Technical Reference Architecture (TRA) and information security standards. The CMS TRA specifies standards for compliance with CMS' Enterprise Architecture, CIO policies, and the CMS Acceptable Risk Safeguards (ARS). CMS technical standards are enforced based on CMS-defined conformance criteria.

Approved by: CTO and CIO

Applicability: CMS-wide; all CMS employees, researchers and organizations conducting business for and on behalf of CMS through contractual relationships when using CMS IT resources

Examples of Technical Standards:

- Technical Reference Architecture (TRA)

Purpose	Other Characteristics
• Articulates the technical architecture of the CMS Processing Environments • Assists all agency business partners in developing to, transitioning to, and maintaining the CMS Processing Environments in accordance with CMS's enterprise technical • May accompany, interpret, or specify requirements for implementing CIO policies, policy aspects, and the CMS Acceptable Risk Safeguards • Serves to accomplish compliance or risk mitigation • May specify rules for using a specific IT Service • Provides guidance to all CMS Expedited Lifecycle (XLC) activities	• Mandatory • The TRA foundation document focuses on technical architecture definition and alignment with Federal Enterprise Architecture (FEA) models. • The CMS TRA supplements focus on engineering detail to aid in consistent development and implementation within CMS environments. • May address specific technologies • Links to templates and other related guidance.

4.4 Guidelines and Best Practices

Guidelines provide guidance and best practices relative to a particular topic. They may accompany, interpret, or provide guidance for implementing CIO policies, or may provide guidance to various CMS IT Life Cycle activities. Guidelines are recommended best practices but are not required to comply with policy. A guideline aims to streamline particular processes according to a set routine or sound practice. By definition, following a guideline is never mandatory. Guidelines are not binding and are not enforced. Some CMS IT guidelines are referred to as "Practices Guides."

A best practice is a technique, method, process, activity, incentive, or reward that is believed to be one of the most effective approaches for delivering a particular outcome when applied to a particular condition or circumstance. The idea is that with proper processes, checks, and testing, a desired outcome can be delivered with fewer problems and unforeseen complications. Best

practices can also be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people. A best practice can be adopted as a guideline.

Both guidelines and best practices are generally high level and reference a parent policy. They may provide alternative approaches and depend on specific technology

Approved by: Applicable Authority

Applicability: CMS-wide; all CMS employees, researchers and organizations conducting business for and on behalf of CMS through contractual relationships when using CMS CIO resources

Examples:

- CIO Library Guidance Hub

4.5 CIO Procedures

CIO procedures consist of step by step instructions to assist workers in implementing policies, standards, and guidelines. Procedures document "how to" accomplish specific IT tasks or use IT services. These procedures may apply at the agency level or they may be localized to reflect the practices or requirements of a specific CMS office, center, group, division, or workgroup.

Approved by: Applicable Authority

Applicability: As stated

Examples:

- Procedure portions of the Risk Management Handbook

5 Policy

5.1 General Principles

The CIO Policy Framework employs the following principles:

- Policy work must be initiated when there is a compelling need for new or revised policy. Triggers may include new technologies, new laws or regulations, or operational or compliance needs that are not appropriately covered by existing policies or guidance.
- CIO policy development may be accomplished via individual workgroups convened to address specific topics. Each workgroup must include appropriate subject matter experts. For more information about policy development workgroups, refer to Section6.1.
- The Division of IT Investment Management Policy (DIIMP) in the IT Capital Planning Group (ICPG), Office of Information Technology (OIT) must provide a central coordination function to ensure consistency and to address policy dependencies.
- The policy development process must be transparent. All CIO policy writing, to the extent possible and practicable, must employ a collaborative effort during development and actively engage an even wider distribution during the policy's review period, to gather a broad perspective of input. Input from stakeholders must be addressed and/or incorporated throughout the process as explained in *Appendix 1: CIO Policy Life Cycle.*
- All CIO policies must be maintained centrally and accessible to all interested stakeholders.
- All published CIO policies must be Section 508 compliant (i.e., fully accessible by disabled and non-disabled individuals).
- Policies and guidance must be implementable and sustainable. Impact risk analysis on both IT systems and end-users must be included in the policy planning and review processes.

- All CIO policies must be kept current through an organized system of change control. At a minimum all CIO policies must be reviewed by the Policy Owner and (if necessary) updated every three (3) years and/or more frequently and/or as significant changes are identified. *See Section 5.4 Document Review and Maintenance Requirements* for policy review criteria and definition of "significant change" as it applies to this policy.
- Any employee or contractor may request consideration of new CIO policies or changes to existing policies.
- The policy development process must be flexible. Circumstances may necessitate the publishing of CIO Directives as a stop-gap to provide immediate guidance while a policy is being developed, vetted, and approved. In other cases, a policy may be established with detailed guidance to be provided at a later time.
- CMS offices/centers/groups/divisions must use this policy or may create a more restrictive policy, but not one that is less restrictive and/or less comprehensive.

5.2 Emergency Policies

In rare cases, such as the need for an emergency policy, the CIO may immediately issue a policy without prior stakeholder comment. The CIO may use this method on an exception basis when:

- The CIO deems it necessary to use sole discretion in determining the policy
- An urgent need exists for immediate notification of a new policy

Even in these rare situations, stakeholders always have the opportunity and responsibility to suggest and request changes. An emergency policy is not an interim policy for it carries the full weight of the CIO and is enforceable.

Please note that issuing a CIO Directive may be more appropriate than issuing an emergency policy when an urgent need exists for immediate notification of urgent information. CIO Directives often serve as a stop-gap to provide immediate guidance while a policy is being developed/updated, cleared, and approved.

5.3 Policy Format, Content, and Style

All CIO policies must conform to standard content, format, and style (font, headers & footers, margins, pagination, etc.), as specified in the *CIO Policy Template and Guide*.

5.4 Initiation and Planning Phase Activities

Identify compelling need for new or updated policy/guidance. Drivers may include new regulatory requirements, technology developments, operational needs, and identification of current issues or gaps.

- The request may come from any CMS employee or contractor but must have the approval of CMS senior leadership prior to moving forward with developing/updating CIO policy
- Determine whether the need should be satisfied by a policy, guideline, directive, standard, or procedure

- Identify policy owner/sponsorship, stakeholders, SMEs, and other workgroup members and their re levant roles
- Prioritize and schedule policy work

5.5 Development Phase Activities

- Create draft policy (or guidelines, standards, procedures, directives); alternatively, revise an existing polic y
- Distribute to workgroup members for initial review and input
- Incorporate initial input
- Division of IT Investment Management & Policy (DIIMP) reviews the DRAFT for content, format and consistency with other existing CIO policies

5.6 CIO Policy Vetting and Clearance Process

The purpose of the CIO Policy Vetting and Clearance Process is to ensure that all CIO policies, standards, and directives authored by CMS (or on behalf of CMS) and approved by the CIO are:

1. Of the highest quality
2. Technically accurate
3. Useful to the intended audience

Vetting and clearance should be appropriate for the type of document under review and should balance the concerns of quality and timeliness. This process promotes consistent clearance procedures throughout CMS that ensure that the highest quality reviews are performed in a reasonable amount of time.

The Division of IT Investment Management & Policy initiates and oversees the formal CIO Clearance Process summarized below. Minimally, all new or substantially revised CIO policies, standards, and directives must have the following three levels of review:

- **Level I Review:** CMS Personnel will be notified to review policy draft and provide comment(s) (if applicable) in the provided CMS CIO Policy Comment Matrix
- **Level II Review:** The Division of IT Investment Management & Policy and CMS CIO will review policy draft and digitally sign to approve updated/refreshed policy. Upon approval, CMS personnel will be notified of approved policy (to include a link to the policy located in the CIO Resource Library at www.CMS.gov)

Once the CIO policy has effectively cleared CMS the CIO Policy Vetting and Clearance Process, the Division of IT Investment Management & Policy places the document under version control and performs rollout activities.

Minor revisions that do not change the substance of a policy (e.g., correcting grammatical or spelling errors, changing links, changing references to other policies or documents, changing position titles, etc.) can be addressed between the Policy Owner and the Division of IT Investment Management & Policy without completing the formal vetting and clearance process.

5.7 Requests for Extensions of Time

Requests for extensions of time to review are made to the Division of IT Investment Management & Policy via email to CIO@CMS.HHS.GOV prior to the review due date and are reviewed and approved/disapproved. It is the responsibility of the Division of IT Investment Management & Policy to

ensure that the extensions are managed timely and that comments received are forwarded to the SME for disposition

5.8 Rollout Activities

The Division of IT Investment Management & Policy has 30 calendar days from the date the policy is signed by the CIO to:

- Post the policy on the CMS website
- Execute policy awareness and communications plan and conduct educational activities, when appropriate
- Initiate Maintenance activities

5.9 Document Review and Maintenance Requirements

Policy owners must review policies at least every three (3) years or more frequently as significant changes that impact the policy are identified. The term "significant change" refers to a change in federal legislation, mandates, directives, executive orders, and/or HHS policy that requires corresponding changes to existing CMS policies.

Document review requirements are a control mechanism to ensure CIO policies are the responsibility of the Policy Owner to review and update on a regular basis and or when there have been significant changes to the policy to ensure accuracy and to identify areas of potential improvement.

To perform a document review, document owners must review the document(s) they own for at least the following:

- Inaccuracies
- Organizational changes affecting the document
- Process changes
- Metric changes
- New or now obsolete external references
- Internal reference document changes including titles
- Links, URLs, or email address changes
- Changes to databases or other data repositories used
- Changes to labor management agreements affecting the document
- Potential areas of improvement
- Incorporation of CIO Directives, as applicable. As CIO Directives are incorporated into policy, the directives are then revoked, as explained in Section 5.4.1 (Policy Revocation).

5.10 Policy Revocation

As part of the maintenance and review process, policies, standards, procedures, and/or guidelines may be identified as out-of-date or no longer needed. They must be revoked via the same process by which they were approved and must be removed from externally accessible web sites upon revocation.

Legacy versions of policies will be stored to ensure:

- compliance with NARA
- accessibility to previous versions policies should requirements reappear
- historical research

6 Stakeholder Involvement

CMS has a major role in CIO policy development and review with the intent of broad coordination and collaboration during CIO policy development and throughout the CIO policy review process.

Critical Partners and Stakeholders must be engaged throughout the CIO policy development process—in both individual and group settings--to ensure that all appropriate perspectives are accounted for and incorporated as feasible in final versions of new or revised policies, standards, guidelines and procedures. DIIMP will notify CMS personnel and CMS contract partners of the various stages in the CIO policy life cycle process.

In general, any CMS employee must be able to provide comments on draft and interim policies, standards, and guidelines on the CMS CIO policy web site. Specific stakeholders may be identified and solicited to provide input and review, while others may be only in the “need to inform” category.

6.1 Policy Development Point of Contact (POC) and/or Policy Subject Matter Expert (SME)

Specific individuals and groups must be identified during the planning and initiation phase of a given policy, standard, or guideline. Membership in policy development workgroups must vary based on the primary content of a policy being developed. DIIMP will provide support to all working groups.

7 Publication and Communication Methods

To ensure timely access and operational effectiveness, finalized CIO policies and other CIO-related reference documents must be published on the CMS CIO Resource Library website. The CMS CIO Resource Library must contain the currently-approved version of all CIO policies, CIO directives, technical standards, guidelines, and procedures. The documents on the CMS CIO Resource Library website must constitute the official electronic repository for agency-wide CIO documents for CMS. *Note: Policies containing sensitive information are subject to restricted distribution and may not be posted on the CMS website.*

8 Roles and Responsibilities

The roles and responsibilities defined below represent the individuals or groups most directly involved in CMS CIO policy development.

Role	Responsibility and Authority
8.1 CMS Chief Information Officer (CIO)	The CIO and Deputy CIO have overall responsibility for IT policy and policy development at CMS that include the following activities: • Reviewing and approving new and revised policies as the final level of governance approval • Permitting employees to participate in policy development workgroups to help develop and review policies and to provide timely comments • When needed, developing and approving policies that are more restrictive than HHS policies but not ones that are less restrictive or less comprehensive • Ensuring that all programs and systems implement the information security and privacy controls required by policy
8.2 CMS Chief Technology Officer (CTO)	The CTO is responsible for the following activities: • Developing the Technical Reference Architecture (TRA) with the support of all components of the Office of Information Technology (OIT) CMS's IT contractors • Approve all changes to the TRA
8.3 Management Officials	Management officials, in their supervisory role, are responsible for the following activities • Ensuring that employees, contractors, interns, etc. participate in the development and the review of CMS CIO policy in a timely manner, as appropriate • Informing users (employees, contractors, interns, etc.) of their rights and responsibilities, including the dissemination of the information in policy
8.4 Division of IT Investment Management & Policy (DIIMP)	DIIMP is responsible for the following activities: • Providing ongoing oversight and direction for the CIO policy program • Providing overall direction for the CIO policy function, including responsibilities for identifying and prioritizing policy needs • Resolving disputes. If conflicting comments are received and cannot be reconciled by the Policy Owner/SME, the conflicts must be escalated to DIIMP for resolution

	• Facilitating and coordinating all CIO Policies developed by CMS or on behalf of CMS • Providing day-to-day support for the policy development function • Determining the potential impact of policies, directives, guidance, best practices, etc. if made publicly available • Planning and executing policy education and awareness efforts • Managing the review and analysis of existing policies, standards, and guidelines for continued applicability and effectiveness on a three-year review cycle • Providing interpretation of current policies in response to inquiries or specific incidents • Providing CMS CIO Policy Matrix for reviewers to provide comments (if applicable).
8.5 Policy Owner/Staff	The Policy Owner (executive leadership) and staff are responsible for the following activities: • Ensuring appropriate stakeholder involvement in policy development • Conducting research and benchmarking for emerging policy development • Development and vetting of policies as described in *Appendix 1: CIO Policy Life Cycle* • Authorizing Level II Review • Communicating updates to all stakeholders • Reviewing policies at least every three (3) years or more frequently as significant changes are identified that impact the policy. The term "significant change" refers to a change in federal legislation, mandates, directives, executive orders, and/or HHS policy that requires corresponding changes to be made to existing CMS policies. • Provides a Summary of Changes that will clearly identify the changes made in the policy draft (e.g. Page, Paragraph, and/or Section, etc.). The Summary of Changes will be located in the beginning of the policy draft.
8.6 Critical Partners and Stakeholders	Critical Partners/Stakeholders are responsible for the following activities: • Reviewing and approving new or revised policies at the Level I review and comment process. • Conducting research and benchmarking for emerging policy development • Composing the subject matter content of CIO • Participating in policy development, vetting, and clearance, as requested
8.7 CMS Employees & Users of CMS IT Resources	Users, including employees, interns, researchers, etc., are responsible for the following activities: • Participating in the development of CIO policy or initiating CIO policy as the subject matter expert (SME), as needed • Responding timely to comments made regarding CIO policy during the CIO Policy Review Process where they are the SME • Providing timely comments during the CIO Policy Review Process and working collaboratively to address issues with the appropriate SME and DIIMP • Familiarizing themselves with any special requirements for accessing, protecting and utilizing data, including but not limited to Privacy Act and Section 508 requirements, copyright requirements, and procurement-sensitive data • Adhering to all conditions set forth in Section 5, Policy

10 Information and Assistance

Direct all questions, comments, suggestions or requests for further information to the Division of IT Investment Management & Policy at CIO@cms.hhs.gov.

11 Applicable Laws/Guidance

HHS OCIO Policy for Information Technology (CIO) Policy Development (HHS-OCIO-2006-004)

Plain Language Act of 2010

12 Reference Documents

Document #	Document Title
N/A	Comments Matrix
N/A	CIO Policy Template and Guide
N/A	Section 508 Policy
N/A	Architecture Change Request

13 Glossary

Term	Definition (or literal translation of acronym)
CIO Policy Document	CIO policy documents include policies, technical standards, directives, guidelines, and procedures that encompass topics related to information technology (IT) as well as information security and privacy
Clearance	The process of obtaining approvals by the appropriate CMS staff members before a CIO policy, standard, or directive is approved for dissemination. Clearance must be appropriate for the type of document under review and should balance the concerns of quality and timeliness. Clearance is not a forum for extensive peer review or for policy debate. Such discussions belong in the pre-clearance phase.
CMS Information Technology (IT) Resources	Includes but is not limited to: staff, facilities, data, documents, laptops/personal computers and related peripheral equipment, software, network and web servers, telephones, facsimile machines, photocopiers, Internet connectivity and access to Internet services, email, and contractor-owned equipment accessing CMS IT resources.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data.
Subject Matter Expert (SME)	A person or persons in a functional area who presents content material regarding the policy subject area.