NEW YORK STATE | Department of Health

Infrastructure and Operations Domain Document

New York State Department of Health (DOH)
Office of Health Insurance Programs (OHIP)

October 23, 2026

Contents

1.0 Introduction 7
- 1.1 Purpose 7
- 1.2 Objectives 7
- 1.3 Authority 8
- 1.4 Scope 8
- 1.5 How This Document is Organized 8
- 1.6 Companion Standards 9
- 1.7 Compliance Tier Framework 10
- 1.8 Compliance and Enforcement 11

2.0 IT Service Management Standard 14
- 2.1 Introduction 14
- 2.2 Objectives 14
- 2.3 ITIL 4 Service Management Framework 15
- 2.4 General Management Practices 15
- 2.5 Service Management Practices 19
- 2.6 Technical Management Practices 26
- 2.7 Management Roles, Responsibilities, and Tools 28
- 2.8 ITSM Tools and Technology 31
- 2.9 Vendor and Partner Integration 31

3.0 Application Integration Standard 37
- 3.1 Introduction 37
- 3.2 Objectives 37
- 3.3 Integration Governance 37
- 3.4 Integration Compliance, Patterns, and Interoperability 38
- 3.5 Integration Quality and Monitoring 41
- 3.6 Integration Change Control 42
- 3.7 Integration Test and Validation 43
- 3.8 Error Handling and Resilience 43

3.9 Documentation and Discoverability 44
4.0 Infrastructure Management Standard 46
4.1 Introduction 46
4.2 Objectives 46
4.3 OHIP Infrastructure Management Strategy 46
4.4 Infrastructure Landscape and Governance Scope 47
4.5 OHIP and Provider Partner Roles and Responsibilities 47
4.6 Operational Governance Standards 50
4.7 Technology Standards 53
4.8 Operational Standards 53
4.9 Operational Controls 54
4.10 Monitoring and Optimization Standards 56
4.11 Incident and Event Management 56
4.12 Performance Standards 57
4.13 Operational Performance Measurement and Reporting 57
4.14 Operational Performance Monitoring 57
5.0 Log Management Standard 58
5.1 Introduction 58
5.2 Objectives 58
5.3 OHIP Logging Governance 58
5.4 Sensitive Data Log Restrictions 60
5.5 Retention Periods 61
6.0 Ongoing Licensing and Support Standard 66
6.1 Introduction 66
6.2 Objectives 66
6.3 Roles and Requirements 67
6.4 Software Approval Process 69
6.5 TCO Assessment 71
6.6 Licensing and Ownership 73
6.7 Support and Maintenance Governance 74
6.8 Security and Compliance Oversight 76
6.9 Integration and Interoperability Requirements 77
6.10 Training and Knowledge Transfer 77
6.11 Contractual Controls and Escalation 78

6.12 Audit and Reporting Requirements 80
6.13 Exit and Transition Planning 82
7.0 Cloud FinOps Standard 84
7.1 Introduction 84
7.2 Objectives 84
7.3 Cloud FinOps Oversight 84
7.4 Financial Transparency and Cost Management 85
7.5 Cloud FinOps Operational Standard 87
8.0 Preferred Operational Tools Standard 89
8.1 Introduction 89
8.2 Objectives 89
8.3 Contractor Tool Use 89
8.4 Maintaining the OHIP Preferred Operational Tools Standard 92
9.0 Contact Information 92
10.0 Revision History 92
Appendices 94
Appendix A: Deliverables and Artifacts 95
Appendix B: Master Requirements Summary 107
Appendix C: Performance Category Definitions 125
Appendix D: ITIL 4 Framework Reference 129
Appendix E: Citations for OHIP MES Logging Requirements 139
Appendix F: ITSM Suggested KPIs 146
Appendix G: Standard Terminology 152
Appendix H: Acronyms 155

Table of Tables

Table 1 – How This Document is Organized 8
Table 2 – Companion Standards 9
Table 3 – Compliance Tier Framework 10

Table 4 – Domain Requirements Summary 11
Table 5 – Integration Methods Minimum Requirements 40
Table 6 – OHIP Enterprise Infrastructure Key Roles 47
Table 7 – Infrastructure Management Environments 51
Table 8 – Log Retention Periods 61
Table 9 – Preferred Operational Tools List 90
Table 10 – ITSM Standard Deliverables and Artifacts 95
Table 11 – Application Integration Deliverables and Artifacts 102
Table 12 – Infrastructure Management Standard Deliverables and Artifacts 103
Table 13 – Ongoing Licensing and Support Standard Deliverables and Artifacts 104
Table 14 – Cloud FinOps Standard Deliverables and Artifacts 105
Table 15 – Master Requirements Summary Table 107
Table 16 – Performance Category Definitions 125
Table 17 – Performance SLA Reporting Elements 126
Table 18 – Governance Functions and Responsibilities for Service Model by Roles .. 127
Table 19 – OHIP Role Mapping 136
Table 20 – Security and Privacy Controls for Information Systems and Organizations Audit and Accountability (AU) Control Family 139
Table 21 – HIPAA Security Rule – 45 CFR Part 164 Subpart C 139
Table 22 – HIPAA Privacy Rule – 45 CFR Part 164 Subpart E 140
Table 23 – Control Element Mapping 141
Table 24 – Authentication Success/Failure Log Fields 142
Table 25 – Privileged Access Log Fields 142
Table 26 – Data Access (PHI/PII/FTI) Log Fields 143
Table 27 – Transactions Log Fields 144
Table 28 – Configuration Changes Log Fields 144
Table 29 – Cross-Cutting Log Fields 145
Table 30 – Continual Improvement Business Suggested KPIs 146
Table 31 – Continual Improvement System Suggested KPIs 146
Table 32 – Continual Improvement Release Suggested KPIs 146
Table 33 – Information Security Management Suggested KPIs 146
Table 34 – Knowledge Management Suggested KPIs 147
Table 35 – Availability Management Suggested KPIs 147

Table 36 – Capacity and Performance Management Suggested KPIs 147
Table 37 – Change Enablement Suggested KPIs 148
Table 38 – Incident Management Suggested KPIs 148
Table 39 – Problem Management Suggested KPIs 149
Table 40 – Release Management Suggested KPIs 149
Table 41 – Service Configuration Management Suggested KPIs 149
Table 42 – Service Desk Management Suggested KPIs 150
Table 43 – Service Request Management Suggested KPIs 150
Table 44 – Service Validation and Testing Suggested KPIs 150

Table of Figures

Figure 1: Infrastructure Management – Standard Structure 48

Issued by:	Finalized:
Office of Health Insurance Programs	10/23/26
Infrastructure and Operations Domain Document	**Owner:** Division of Operations and Systems (DOS) and Chief Technology Office (CTO)

1.0 Introduction

1.1 Purpose

The Office of Health Insurance Programs (OHIP) Solution Delivery Domain Document establishes technical, operational, and quality standards governing how OHIP Medicaid Enterprise Systems (MES) solutions are designed, developed, tested, and delivered. This domain standard ensures all contractors implementing or enhancing OHIP systems do so with consistency, auditability, and in compliance with federal certification requirements.

The OHIP standards establish the mandatory technical, operational, and security requirements for New York State (NYS) to remain compliant with federal regulations under 42 CFR § 433.112, qualifying the state for enhanced Federal Financial Participation (FFP). Deliverables and artifacts associated with this standard can be found in Appendix A.

1.2 Objectives

The primary objectives of this domain standard are to:

- Establish a comprehensive Information Technology (IT) service management framework grounded in IT Infrastructure Library® (ITIL) 4 for delivering, managing, and continually improving all IT services across the OHIP MES (Section 2.0).
- Define mandatory requirements for application integration, including Application Programming Interface (API) governance, national data exchange standards (Health Level 7 [HL7], Fast Healthcare Interoperability Resources [FHIR] R4, X12 Electronic Data Interchange [EDI]), Event-Driven Architecture (EDA), and integration resilience (Section 3.0).
- Provide a framework for the adoption, implementation, and management of cloud infrastructure services across Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) models, with SaaS as the preferred delivery model (Section 4.0).
- Ensure regulatory and policy compliance for log management by establishing uniform requirements for audit event logging, sensitive data protection, and log retention (Section 5.0).
- Govern the procurement, licensing, support, and lifecycle management of all third-party software, tools, and solutions integrated into the MES environment (Section 6.0).
- Achieve financial transparency and accountability for all cloud expenditures through Cloud FinOps practices, including cost allocation, usage monitoring, and optimization (Section 7.0).

- Standardize the operational toolset across all MES Contractors to ensure compatibility, interoperability, and alignment with OHIP's technology stack (Section 8.0).
- Ensure coordinated multi-vendor service delivery through standardized roles, escalation procedures, and integration with OHIP's ITSM platform.

1.3 Authority

The NYS Department of Health (DOH) is the primary authority overseeing the health, safety, and well-being of New Yorkers since 1901. The Department delegates direct operational control and administrative responsibility for the Medicaid Program to the OHIP. Title 11 of the NYS Social Services Law enables OHIP to establish and enforce the standards necessary to administer the State's Medicaid Program. This foundational authority, further supported by the broad regulatory powers vested in the Commissioner of Health by the NYS Public Health Law, enables OHIP to create comprehensive policies and procedures required for the effective, secure, and compliant operation of the MES.

For health information standards, compliance with HIPAA regulations is mandatory, with specific New York enforcement through the NYS Public Health Law. Article II of the NYS Technology Law mandates security policies that comply with both State and federal requirements. The NYS Information Security Breach and Notification Act ensures entities managing sensitive data adhere to privacy and security protocols.

OHIP applies these standards across both hybrid and non-hybrid entities in the Department, ensuring robust protection for all sensitive information including Protected Health Information (PHI), Personally Identifiable Information (PII), Medicaid Confidential Data (MCD), IRS Federal Tax Information (FTI), and other regulated data, aligning with federal and State mandates for data integrity, security, and privacy.

1.4 Scope

This Standard applies to specific contractually negotiated activities between OHIP and existing contracts and to new procurements/contracts identified as part of the evolving MES Roadmap.

The Contractor **MUST** demonstrate how the requirements of this standard will be met within their specific system context. Where system-specific constraints exist, the Contractor **MUST** document those constraints and propose alternative approaches for OHIP approval that achieve an equivalent level of compliance and rigor. Proposed alternatives do not relieve the Contractor of any obligation under this standard unless OHIP provides written approval through the Standards Deviation Request (SDR) process defined in Section 1.7.1.

1.4.1 Multi-System Applicability

OHIP operates a diverse portfolio of systems that vary in architecture, technology stack, and operational maturity. This standard is platform-agnostic in its requirements while acknowledging that implementation approaches can differ across OHIP's portfolio of systems.

1.5 How This Document is Organized

This document encompasses multiple related OHIP standards. Each component standard is presented as a dedicated section (Sections 2 through 8). An Appendix and Master Requirements Summary Table appears at the end of the document.

Table 1 – How This Document is Organized

Section	Domain Area

Section 2.0	Information Technology Service Management (ITSM) Standard
Section 3.0	Application Integration Standard
Section 4.0	Infrastructure Management Standard
Section 5.0	Log Management Standard
Section 6.0	Ongoing Licensing and Support Standard
Section 7.0	Cloud FinOps Standard
Section 8.0	Preferred Operational Tools Standard

1.6 Companion Standards

The following external OHIP standards directly govern, extend, or bound activities described in this domain standard. Standards previously cited as companions that have been consolidated within this document are now cross-referenced by section number. All references to individual component standards within Sections 2–8 **SHOULD** be read as references to that section of this document.

> 📝 ***Note:*** *Internal cross-references between sections of this document (Sections 2 through 8) are provided within each section's introduction. The table below lists only external companion standards that are maintained as separate documents.*

Table 2 – Companion Standards

OHIP Standard	Domain	Scope Relationship
OHIP Solution Development Life Cycle (SDLC) Standard	Solution Delivery	Governs the full software development lifecycle for all MES solutions, including requirements management, code standards, policy and business rules, test management, and release management. Supports Waterfall, Agile, and Hybrid methodologies and integrates security, privacy, and architecture oversight into every phase of delivery.
OHIP Data Architecture and Naming Standard, OHIP Database Design Standard, OHIP Data Lakehouse Architecture Standard	Data and Information Management	Governs all aspects of data as a strategic asset, including naming conventions, database design, data conversion, and Lakehouse architecture. Ensures compliance with HIPAA, MITA, and applicable federal regulations while enforcing interoperability standards, and lifecycle management across all OHIP systems.
OHIP Security and Privacy Compliance Standard	Security, Privacy and Compliance	Governs adherence to OHIP's Security and Privacy Controls Baseline for all systems that create, process, transmit, or store OHIP data. Establishes requirements for System Security and Privacy Plans (SSPP), legally binding data handling agreements, and a centralized compliance reference repository accessible to all internal and external stakeholders.
OHIP Project Management Standard, OHIP Project Change Control Standard, OHIP Technical Change Control Standard, OHIP Contract Management Standard	Program and Project Management	Governs program and project management across the MES program, including project change control, technical change control, transition-in and transition-out planning, schedule and risk management, and the master plans that this domain's operational activities execute.

1.7 Compliance Tier Framework

This standard uses three compliance tiers applied consistently throughout all sections and in the Master Requirements Summary in Appendix B. Every requirement has been individually vetted against enforceability, technical precision, and practicality before receiving its tier assignment. Tier designations appear in throughout the document and in the Tier column of Appendix B.

Table 3 – Compliance Tier Framework

Tier	Type	Definition
MUST	Mandatory	**MUST** requirements are mandatory. Violation constitutes a material breach. Any deviation requires submission of a formal SDR and written approval from the OHIP IT Standards Team prior to implementation. **MUST** requirements are binding on all procurement activities and contracts and are subject to audit as part of CMS Streamlined Modular Certification (SMC) reviews.
SHOULD	Strong Recommendation	**SHOULD** requirements are strongly recommended. Exceptions **MAY** be permitted under specific documented circumstances. Any deviations require written justification to the OHIP Project Manager for approval and **MUST** be documented in the project deviation log. **SHOULD** requirements are cited as expected practice in procurement activities and contracts. An SDR is not required; however, all deviations **MUST** be affirmatively justified in writing.
MAY	Permitted Option	**MAY** requirements denote a permitted option or permissible alternative at the discretion of the Contractor or OHIP. When a **MAY** option includes stated conditions, those conditions **MUST** be satisfied before the option **MAY** be exercised. **MAY** statements are informational within procurement activities and contracts and do not require prior approval or deviation documentation.

1.7.1 Standards Deviation Request (SDR) Process

A SDR is the formal mechanism by which a Contractor seeks approval to deviate from a **MUST** requirement prior to implementation. An SDR does not apply to **SHOULD** or **MAY** requirements. The SDR process is prospective: it **MUST** be completed and approved prior to the deviating approach is implemented. Retroactive SDRs will not be accepted and do not cure a breach.

The Contractor **MUST** submit a completed SDR to the OHIP IT Standards Team for any proposed deviation from a **MUST** requirement. An SDR is a prospective request: it **MUST** be submitted and approved by OHIP before the Contractor implements any non-compliant approach. The SDR package **MUST** include:

- **Requirement ID:** the specific requirement identifier from Appendix B
- **Proposed Alternative:** a complete description of the approach to be used instead of the **MUST** requirement
- **Technical Justification:** documented rationale explaining why the **MUST** requirement cannot be met
- **Risk Assessment:** identification of risks introduced by the deviation and their likelihood and impact
- **Mitigation Controls:** specific measures that will reduce or compensate for identified risks

- **Proposed Timeline:** target date for achieving full compliance, if the deviation is temporary

OHIP will review the SDR and issue a written approval or denial within ten (10) business days of receipt of a complete submission. Incomplete submissions will be returned without review. Approved SDRs are logged in the OHIP Deviation Register with the effective date, any conditions attached to the approval, and the anticipated compliance date where applicable. Conditional approvals **MUST** be re-reviewed at the specified review date.

> 📝 ***Note:*** *OHIP reserves the right to revoke an approved SDR if circumstances change, if conditions are not met, or if the deviation creates unforeseen risk to program integrity, federal compliance, or data security. Revocation of an SDR is subject to reasonable notice except where urgent risk requires immediate action.*

1.7.2 Domain Requirements Summary

The following table summarizes requirement counts across the seven component standards. A complete master listing of all requirements with individual tier assignments appears in Appendix B.

Table 4 – Domain Requirements Summary

Standard	Section	ID Range	MUST	SHOULD	MAY	Total
ITSM Standard	Sec. 2	INFRA-0001 – INFRA-0059	46	12	1	59
Application Integration Standard	Sec. 3	ARCH-0001 – ARCH-0050	44	6	0	50
Infrastructure Management Standard	Sec. 4	INFRA-0060 – INFRA-0094	30	5	0	35
Log Management Standard	Sec. 5	INFRA-0095 – INFRA-0120	25	1	0	26
Ongoing Licensing and Support Standard	Sec. 6	INFRA-0121 – INFRA-0161	34	6	1	41
Cloud FinOps Standard	Sec. 7	INFRA-0162 – INFRA-0186	19	5	1	25
Preferred Operational Tools Standard	Sec. 8	INFRA-0187 – INFRA-0200	12	2	0	14
		Total	**210**	**37**	**3**	**250**

Table key: **MUST** = mandatory. **SHOULD** = strongly recommended. **MAY** = permitted option.

1.8 Compliance and Enforcement

This section establishes the obligations, rights, and remedies that govern compliance with this standard throughout the contract term. This standard is incorporated into the Contract, and OHIP reserves the right to update it during the term; the version in effect at the time of performance applies to the requirements it sets. The compliance and enforcement provisions in this section supplement, and do not replace, the remedies and enforcement terms of the governing Contract.

1.8.1 Applicability and Effective Date

The Contractor **MUST** comply with this standard and all applicable laws, regulations, and funding requirements. Compliance is required from the effective date of the Contract or Contract Amendment.

1.8.2 Updates to the Standard

OHIP reserves the right to amend this standard at any time. OHIP will use reasonable efforts to provide at least thirty (30) days' notice before enforcement of substantive changes. The Contractor **MUST** implement changes by the designated effective date.

For changes required by law, funding conditions, or urgent security risks, OHIP reserves the right to designate an earlier effective date. The Contractor **MUST** comply by that date regardless of other project commitments.

Within ten (10) business days of receiving notice of a substantive change, the Contractor **MUST** submit an impact assessment to OHIP and, if applicable, a proposed implementation plan including any requested cost or schedule adjustments. Acceptance of adjustments is at OHIP's sole discretion.

1.8.3 Monitoring, Audit, and Records Retention

OHIP and its designees reserve the right to audit the Contractor's and subcontractors' compliance with this standard upon ten (10) business days' notice, or less for cause or urgent security issues. The Contractor **MUST** provide reasonable access to relevant facilities, systems, records, and personnel upon request.

The Contractor **MUST** retain records evidencing compliance with this standard for at least seven (7) years from creation, or as otherwise required by law or funding requirements, whichever is longer.

1.8.4 Notification of Non-Compliance and Security Events

The Contractor **MUST** notify OHIP in writing within three (3) business days upon identification of any non-compliance with this standard.

Where non-compliance materially impacts the confidentiality, integrity, or availability of OHIP systems or data, or could result in legal or funding exposure, notification **MUST** be made immediately and no later than twenty-four (24) hours after discovery.

All notifications **MUST** describe: the nature and scope of the issue, root cause if known, immediate containment steps taken, and a proposed Corrective Action Plan (CAP) with timeline.

1.8.5 Corrective Action Plan (CAP)

Within ten (10) business days of notice, whether by the Contractor or OHIP of any non-compliance with this standard, the Contractor **MUST** provide a CAP acceptable to OHIP. The CAP **MUST** include defined milestones, responsible parties, and due dates for each remediation step.

OHIP reserves the right to impose or modify a CAP where the Contractor's proposed plan is insufficient.

1.8.6 Remedies and Enforcement

In addition to any other rights and remedies available under the Contract or applicable law, OHIP reserves the right to exercise any or all of the following remedies upon Contractor non-compliance:

- Withhold payments due under the Contract
- Assess service credits or liquidated damages as set forth in the Contract
- Suspend or limit the Contractor's system access

- Require removal of personnel or sub-contractors
- Require re-performance of non-compliant work at no additional cost to OHIP

Remedies are cumulative and can be exercised concurrently. OHIP can also refer matters to oversight bodies or regulators as required by law or policy.

1.8.7 Exceptions and Risk Acceptance

An exception is distinct from a SDR (see Section 1.7.1). An SDR is a prospective mechanism, it is submitted before a non-compliant approach is adopted. An exception, by contrast, applies where strict compliance is not technically feasible after implementation has begun, or where an existing system or constraint prevents full compliance by the effective date. OHIP will evaluate each exception request on its individual merits and will not grant exceptions that would violate applicable law, federal funding requirements, or CMS certification conditions.

To request an exception, the Contractor **MUST** submit a written request to OHIP that includes: a risk assessment identifying the nature and severity of non-compliance risk; proposed mitigation measures that reduce that risk to an acceptable level; and a proposed timeline either for achieving full compliance or for implementing a permanent alternative solution.

Exceptions are subject to the following conditions:

- Exceptions are time-bound—they expire at the date specified in the approval unless renewed by OHIP in writing.
- Exceptions are non-transferable—they apply only to the specific Contractor, system, and circumstance described in the request.
- Exceptions require OHIP's prior written approval before the non-compliant approach is adopted or continued.
- No exception will be granted that would violate applicable law, federal funding requirements, or OHIP policy.
- OHIP can revoke an approved exception at any time upon material changes in risk, regulatory requirements, or program needs.

> 📝 ***Note:*** *Approved exceptions are tracked in the OHIP Deviation Register alongside approved SDRs. Both represent formal acknowledgment by OHIP of a documented departure from standard requirements. Neither constitutes a waiver of OHIP's rights under the Contract.*

2.0 IT Service Management Standard

2.1 Introduction

The ITSM Standard establishes the mandatory framework for delivering, managing, and continually improving all IT services supporting the OHIP MES. In a multi-vendor environment where Contractors share responsibility for systems that New York's Medicaid beneficiaries, providers, and program administrators depend on daily, disciplined service management is the mechanism that ensures consistent service quality, coordinated incident response, and accountable performance across organizational boundaries.

This standard is grounded in ITIL Version 4, the globally recognized framework for ITSM, adapted to the regulatory and operational context of NYS Medicaid. It requires every MES Contractor to implement standardized practices across three categories: General Management Practices (Section 2.4), which govern cross-cutting disciplines such as continual improvement, risk management, and knowledge management; Service Management Practices (Section 2.5), which govern the core operational disciplines of incident management, change enablement, release management, and service level management; and Technical Management Practices (Section 2.6), which govern deployment, infrastructure, and solution development activities.

The standard further defines the management roles each Contractor must fill (Section 2.7), the ITSM tooling and integration requirements (Section 2.8), and the vendor coordination framework that governs how Contractors interact with each other and with OHIP in a shared-service environment (Section 2.9).

Compliance with this standard is a prerequisite for CMS SMC and for OHIP's sustained eligibility for enhanced FFP. These requirements apply to all Contractors from contract award through transition-out, regardless of the cloud service model or SDLC methodology employed. Associated deliverables and artifacts for this standard are located in Appendix A.

2.2 Objectives

The primary objectives of this Standard are to:

- Establish a single, comprehensive framework for designing, delivering, and managing all IT services to ensure consistency and standardization across the OHIP enterprise.
- Improve service quality, operational excellence, and customer satisfaction by adopting the ITIL Version 4 as the official service management framework for the MES.
- Provide clear guidelines and processes for managing IT operations in a complex, multi-vendor environment to ensure seamless service delivery and clear accountability.
- Standardize ITSM tooling for service requests, assets, and incidents by migrating all related processes to OHIP’s preferred ITSM solution.[1]

[1] For more information, refer to Section 8.0.

2.3 ITIL 4 Service Management Framework

2.3.1 Key ITIL 4 Concepts Applied in This Standard

OHIP's approach to service management incorporates the core components of the ITIL 4 Service Value System. This system describes how all parts of an organization work together to facilitate value creation through a holistic model that includes guiding principles, governance, a service value chain, defined practices, and continual improvement.

The Seven Guiding Principles of ITIL 4 inform all OHIP service management decisions. The Contractor **MUST** incorporate these principles into their service management approach to ensure alignment with OHIP's operational philosophy:

- Focus on Value
- Start Where You Are
- Progress Iteratively with Feedback
- Collaborate and Promote Visibility
- Think and Work Holistically
- Keep It Simple and Practical
- Optimize and Automate

The Four Dimensions Model ensures a holistic approach to service management by requiring consideration of Organizations and People, Information and Technology, Partners and Suppliers, and Value Streams and Processes. Every aspect of service management **MUST** address all four dimensions to ensure effective value delivery.

ITIL 4 defines thirty-four (34) practices organized into General, Service, and Technical Management categories. This standard adopts the practices most relevant to OHIP's multi-vendor environment, with detailed requirements specified in Sections 2.4, 2.5, and 2.6.

2.3.2 OHIP-Specific Adaptations

While this standard is grounded in ITIL 4, specific adaptations have been made for OHIP's unique operating environment. For instance, multi-vendor coordination protocols are established in Section 2.9 to govern how the Contractor interacts and collaborates across system boundaries.

This standard also aligns with Office of IT Services (ITS) Enterprise Operations Standards to ensure OHIP service management activities integrate with broader state IT governance. Furthermore, all service management activities **MUST** comply with federal and state regulatory requirements, including HIPAA and applicable NYS regulations governing health information systems.

For detailed reference information on the ITIL 4 framework, including comprehensive descriptions of all concepts mentioned above, please refer to Appendix D: ITIL 4 Framework Reference.

2.4 General Management Practices

This section covers general management practices relevant to OHIP operations. These practices are adapted from business management domains and support effective service delivery. The Contractor **MUST** implement these practices in accordance with OHIP requirements.

2.4.1 Continual Improvement

The Contractor **MUST** align practices and services with changing business needs through the ongoing improvement of products, services, and practices. The scope of this practice includes, but is not limited to:

- Improvement planning and tracking
- Value stream mapping and optimization
- Performance analysis and gap identification
- "Lessons learned" capture and dissemination
- Improvement initiative management and reporting

The Contractor **SHOULD** execute the seven steps of Continual Improvement related to the components of their solution. The Contractor **MUST** define the service improvements in collaboration with OHIP, Business Support Services (BSS), and Technical Advisory Services (TAS). The Contractor **MUST** capture data for the services at a frequency agreed upon with OHIP. The Contractor **MUST** schedule and implement service improvements and analyze and present data for the services per a cadence cycle mutually agreed upon with OHIP.

Suggested KPIs for these practices (Continual Improvement Business, Continual Improvement System, and Continual Improvement Release) are provided in Appendix F, Table 30, Table 31, and Table 32 respectively.

2.4.2 Information Security Management

The Contractor **MUST** operate an Information Security Program that protects the confidentiality, integrity, and availability of OHIP information systems, business processes, and facilities through administrative, physical, and technical controls commensurate with assessed risk, and that complies with all applicable security and privacy laws and regulations. Detailed security and privacy requirements are governed by the OHIP Security, Privacy, and Compliance Domain Document.[2]

Suggested KPIs for these practices (Information Security Management) are provided in Appendix F, Table 33.

2.4.3 Relationship Management

The Contractor **MUST**:

- Identify OHIP's key stakeholders and maintain a current map of stakeholder roles, interests, and engagement channels at both the strategic and operational levels.
- Maintain effective relationships with OHIP stakeholders through regular communication, stakeholder engagement activities, satisfaction surveys, and proactive issue resolution.

2.4.4 Supplier Management

The Contractor **MUST** manage its suppliers and subcontractors to ensure uninterrupted provision of quality products and services. This includes maintaining a current inventory of the suppliers and

[2] For more information, refer to the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard.

subcontractors supporting the OHIP solution, flowing down the applicable requirements of this standard to them, and monitoring their performance against agreed obligations. OHIP Technology operates as a multi-sourced ecosystem delivering value through differentiated services and vendor partners, such as TAS, BSS, and other Contractors; contracts are centrally managed by the OHIP Contract Management team.

The Contractor **MUST** report Service Level Agreement (SLA) breaches to the OHIP Contract Management team to support validation and assessment of LD.

2.4.5 Knowledge Management

The Contractor **MUST**:

- Create and maintain Standard Operating Procedures (SOPs) for the Service Desk, stored within OHIP's ITSM Knowledge Repository.
- Maintain knowledge assets in OHIP's ITSM Knowledge Repository so that current, accurate knowledge is accessible to authorized users across the program.

Suggested KPIs for these practices (Knowledge Management) are provided in Appendix F, Table 34.

The Contractor **SHOULD**:

- Create Training Plans and training artifacts related to the solution being implemented.

2.4.6 Organizational Change Management

Organizational Change Management (OCM) is governed by the OHIP Program and Project Management Domain Document. In support of service management, the Contractor **MUST** enable adoption of service changes through people-focused approaches, stakeholder communication and engagement, assessment of people-related risks, training and awareness, and measurement of adoption in alignment with the PPM Domain Document.

2.4.7 Project Management

The Contractor **MUST** plan, direct, and motivate all the resources used by a project to achieve the project objectives within the expected scope, schedule, budget, and quality.

The Contractor **SHOULD** adhere to the OHIP Program and Project Management Domain Document, Project Management Standard[3] for all approved projects and initiatives, providing regular status reports, managing risks and issues, and ensuring deliverables meet agreed-upon criteria.

> 📝 ***Cross-Reference:*** *OCM (2.4.6) and Project Management (2.4.7) are program-level disciplines governed by the OHIP Program and Project Management Domain Document. These ITIL practices are included here for service-management completeness; the governing requirements, plans, and deliverables are defined in PPM and are not redefined in this document.*

[3] For more information, refer to the OHIP Program and Project Management Domain Document.

2.4.8 Risk Management

To support risk management, the Contractor **MUST**:

- Identify, assess, and control risks to its solution and services throughout the contract term, maintaining a current risk register that records each risk's likelihood, impact, owner, and mitigation status.
- Analyze the business impact of identified risks and coordinate with OHIP and other stakeholders to mitigate them, escalating risks to OHIP in accordance with agreed thresholds and reporting cadence.

2.4.9 Service Financial Management

To support the organization's strategy and plans for service management, the Contractor **MUST**:

- Track and manage the financial resources and investments associated with its services so that costs are controlled and attributable.
- Provide any required financial information related to their services to support OHIP's financial management processes, including cost tracking, and providing data for charge-back or show-back models if applicable.[4]

> 📋 ***Cross-Reference:*** *Cloud-specific financial management and cost optimization are governed by Section 7.0.*

2.4.10 Strategy Management

The Contractor **SHOULD** align its services, improvement initiatives, and roadmap with OHIP's documented strategic goals and priorities, and **SHOULD** be able to demonstrate that alignment in its planning artifacts and in periodic reviews with OHIP.

2.4.11 Portfolio Management

The Contractor **MUST** provide OHIP with accurate, current information on its service portfolio including service performance, costs, and dependencies to support OHIP's enterprise portfolio-management decisions, and **MUST** manage the mix of its own programs, projects, products, and services to deliver the outcomes committed to OHIP within agreed funding and resource constraints.

2.4.12 Architecture Management

For architecture management, the Contractor **MUST**:

- Maintain current architecture documentation for its solution that shows its components and their interrelationships, consistent with the OHIP MES Standards Framework.
- Adhere to the OHIP MES Standards Framework and an approved Configuration Management Plan.[5]

---

[4] For more information, refer to Section 7.0, the OHIP Program and Project Management Domain Document, and the OHIP Solution Delivery Domain Document, SDLC Standard.
[5] For more information, refer to the OHIP Program and Project Management Domain Document, Technical Change Control Standard and the OHIP Solution Delivery Domain Document.

- Seek OHIP approval for all architectural decisions, designs (including process flows) through the OHIP EA governance process.

2.4.13 Measurement and Reporting

Measurement and reporting support transparency and informed decision-making. For measurement and reporting, the Contractor **MUST**:

- Measure, monitor, and report on the performance of their responsibilities as defined in this standard and individual contracts.
- Provide accurate, timely reports in the format and at the cadence specified by OHIP.

2.4.14 Workforce and Talent Management

To support the management of resources, the Contractor **MUST** ensure:

- Staff with the appropriate skills and knowledge are assigned to the roles required to meet its obligations.[6]
- Their staff are appropriately qualified and trained for their roles.

2.5 Service Management Practices

This section describes service management practices that are central to ITSM operations. These practices are adapted from traditional ITSM domains and are specific to technology service management.

The Contractor **SHOULD**:

- Roles are filled as defined in Section 2.7 with qualified staff, and depending on contract size and complexity, roles **MAY** be combined with OHIP approval.

2.5.1 Availability Management

For availability management, the Contractor **MUST** ensure that services deliver agreed levels of availability to meet the needs of its customers and users.

Capacity and performance are critical capabilities within availability management. The Contractor **MUST** establish mechanisms to capture and report agreed-upon capacity and performance metrics to the Department in accordance with contractual agreements.

The Maintenance and Operations (M&O) Plan describes a framework detailing methodologies, processes, and schedules to facilitate efficient and effective management of day-to-day operations including strategies for ensuring availability. M&O refers to the continuous process of keeping systems up to date, efficient, and functional. It covers routine maintenance, such as necessary break/fixes, operational updates, and/or upgrades to software and hardware components. Software **MUST** be maintained at the N-1 version where N is the most current version. Operational activities include the day-to-day running of the system, such as ensuring data is properly processed and stored, managing user access and security, and troubleshooting any issues that arise in accordance with the approved SLAs.

---

[6] For detail on the staff qualification process, refer to the OHIP Program and Project Management Domain Document, Contract Management Standard.

M&O includes correction of previously released functionality that contains issues, problems, bugs, or defects in the solution.

Suggested KPIs for these practices (Availability Management) are provided in Appendix F, Table 35.

2.5.2 Business Analysis

The Contractor **MUST** participate in business analysis activities as required by OHIP, providing technical and domain expertise to analyze business elements or systems, identify needs and improvement opportunities, and recommend solutions that deliver value to stakeholders. This includes gathering and documenting business requirements, analyzing and modeling business processes, developing business cases for change, translating business needs into functional and non-functional requirements, and evaluating potential solutions to ensure that new or changed services meet business needs.

2.5.3 Capacity and Performance Management

The Contractor **MUST** ensure that services achieve agreed and expected performance levels, satisfying current and future demand in a cost-effective way. This includes capacity planning and forecasting, resource optimization, performance monitoring and analysis, and capacity reserves management.

The Contractor **MUST** execute performance, stress, and load testing to establish benchmarks, upper performance limits, and maximum operating capacity. The Contractor **MUST** make any necessary modifications to ensure the solution reaches acceptable performance levels in a production environment. The System Enhancement and Upgrade Report provides an assessment and overview of current system performance.

Suggested KPIs for these practices (Capacity and Performance Management) are provided in Appendix F, Table 36.

2.5.4 Change Enablement

The Contractor **MUST** establish and document the approaches and processes for managing service and product changes, maximizing the number of successful changes by ensuring risks are properly assessed, authorizing changes to proceed, and managing the change schedule. The Contractor **MUST**:

- Assess and mitigate risks, including information security risks.
- Coordinate deployment schedules to eliminate maintenance conflicts.
- Document changes to configuration items.

Managing three change types:[7]

- **Standard**: Recurring, low-risk, pre-approved changes
- **Normal**: Changes requiring full assessment and authorization
- **Emergency**: Changes to fix critical incidents or address high-priority security vulnerabilities

[7] For more information, refer to the OHIP Program and Project Management Domain Document, Technical Change Control Standard.

Change Enablement applies to all Configuration Items. The Contractor **MUST** initiate the Technical Change Request in OHIP's solution which **MUST** be approved by OHIP. A ten-day (10) minimum lead time is required for normal changes.

The following are required by OHIP to be under change and configuration control:

- Any changes to infrastructure, regardless of environment
- Any changes to the business application in the Stage and PROD environments
- Any changes to Commercial Off-The-Shelf (COTS) products, including database products.

A Change Request is required for each change to ensure that any potential change to the security boundary is documented and approved. The Contractor **MUST** perform a post-implementation test on each change to verify that security features and boundaries are unchanged.[8]

Suggested KPIs for these practices (Change Enablement) are provided in Appendix F, Table 37.

> 📋 ***Cross-Reference:*** *Integration-specific change control is governed by Section 3.6. Infrastructure-specific change control is governed by Section 4.9.1.*

2.5.5 Incident Management

The Contractor **MUST**:

- Minimize the negative impact of incidents by restoring normal service operation as quickly as possible.
- Be responsible for incident detection, logging, categorization, prioritization, escalation, diagnosis, resolution, and closure.
- Manage all incidents using its OHIP-approved Incident Management Plan.
- Emphasize user experience, satisfaction, and automation where appropriate.

Suggested KPIs for these practices (Incident Management) are provided in Appendix F, Table 38.

> 📋 ***Cross-Reference:*** *Integration monitoring and automated incident creation are governed by Section 3.5. Infrastructure incident and event management is governed by Section 4.11.*

2.5.6 IT Asset Management (ITAM)

The Contractor **MUST** plan and manage the full life cycle of all IT assets to maximize value, control costs, manage risks, and meet regulatory and contractual requirements. This includes tracking and managing all hardware, software, cloud, and license assets; managing software license compliance; optimizing asset procurement, utilization, and retirement; and performing regular asset audits.

The Contractor **MUST** manage all IT assets associated with their solution, maintaining accurate records of asset location, ownership, and status. This includes managing software licenses to ensure compliance

[8] For more information, refer to the OHIP Program and Project Management Domain Document, Technical Change Control Standard, the OHIP Solution Delivery Domain Document, Release Management Standard, and the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard.

and providing asset information to support other ITSM practices such as Change and Configuration Management. Records of configuration-controlled changes to the information system **MUST** be retained for at least three (3) years, unless a longer period is mandated by OHIP.[9]

2.5.7 Monitoring and Event Management

The Contractor **MUST** systematically observe services and service components to detect, filter, categorize, and respond to events. The Contractor **MUST** perform event detection, logging, categorization, correlation, prioritization, escalation, resolution or workaround implementation, closure, and closure communication for the IT solution implemented and supported. Event detection, logging, and categorization **MUST** be automated to the greatest extent feasible.[10]

> 📝 ***Cross-Reference:*** *Integration-specific logging is governed by Section 3.5. Enterprise log management requirements including retention and sensitive data restrictions are governed by Section 5.0.*

2.5.8 Problem Management

For problem management, the Contractor **MUST**:

- Reduce the likelihood and impact of incidents by identifying actual and potential causes of incidents and managing workarounds and known errors.
- Be responsible for problem detection, logging, categorization, prioritization, investigation, diagnosis, resolution, and communication.
- Emphasize proactive problem identification, root cause analysis, and known error management.

These processes **MUST** be detailed in the Problem Management Plan.

Suggested KPIs for these practices (Problem Management) are provided in Appendix F, Table 39.

2.5.9 Release Management

Release Management makes new and changed services and features available for use, including release planning, scheduling, and coordination; managing the build, test, and deployment of releases; and coordinating with Change Enablement and Deployment Management.

The Contractor **MUST** produce and maintain the Release Plan, including a release schedule and release notes detailing features, known errors and limitations, infrastructure and software components to be deployed, and tests to be conducted with expected outcomes.[11] The Contractor **MUST** manage the entire Release and Deployment Management life cycle in coordination with OHIP stakeholders and vendor partners for higher environments.

The Contractor **MUST** utilize static and dynamic code scan software on code packages labeled for production release before any production release. Scan reports **MUST** be made available to OHIP before

---

[9] For more information, refer to Section 5.0.
[10] For more information, refer to Section 5.0.
[11] For more information, refer to the OHIP Solution Delivery Domain Document, Release Management Standard.

every production release. Performance testing **MUST** be executed and results **MUST** be made available to OHIP before every production release.[12]

Suggested KPIs for these practices (Release Management) are provided in Appendix F, Table 40.

> 📝 ***Cross-Reference:*** *Infrastructure-level change control for deployments is governed by Section 4.9.1.*

> 📝 ***Cross-Reference:*** *Release planning and the Release Plan, release schedule, and release notes are governed by the Solution Delivery Domain Document, Release Management Standard (Section 7.0); the static and dynamic code-scanning requirements are governed by the Solution Delivery Domain Document, Code Standard (Section 5.0). This section addresses the ITIL operational coordination of release and deployment activities and does not redefine the Release Plan artifact or the code-scanning requirements.*

2.5.10 Service Catalog Management

The Contractor **MUST** maintain a Service Catalog containing accurate details reflecting the status, possible interactions, and mutual dependencies of all current services and those being prepared to run operationally. This includes defining and maintaining service descriptions, ensuring the catalog is accurate and available to the relevant audience, and aligning the catalog with business and user needs. This catalog acts as an input to the Enterprise Level Service Catalog.

> 📝 ***Cross-Reference:*** *The integration catalog defined in Section 3.9 complements this enterprise Service Catalog.*

2.5.11 Service Configuration Management

The Contractor **MUST** ensure that accurate and reliable information about the configuration of services and the Configuration Items that support them is available when and where needed.

The Contractor **MUST** create and execute an approved Configuration Management Plan addressing configuration planning, Configuration Management Database (CMDB) management, Configuration Item identification, configuration audits, and reporting on configuration performance. The Contractor **MUST** maintain a CMDB within a service management tool supporting Incident, Problem, and Change Control capabilities. Older versions of approved baseline configurations **MUST** be maintained and made available for review and rollback if needed.

Suggested KPIs for these practices (Service Configuration Management) are provided in Appendix F, Table 41.

[12] For more information, refer to the OHIP Solution Delivery Domain Document, Test Management Standard.

2.5.12 Service Continuity Management

The Contractor **MUST** ensure that the availability and performance of services are maintained at sufficient levels in the event of a disaster. The Contractor **MUST**:

- Develop and maintain a Business Continuity and Disaster Recovery (BC/DR) Plan for the components of their solution, based on Enterprise BC/DR requirements.
- Conduct Business Impact Analysis (BIA) and risk assessments.
- Develop and document recovery strategies and plans.
- Regularly test continuity and recovery plans.
- Manage and coordinate responses to disaster events.

Capacity Management assists with the assessment of business impact and risk and determines the capacity needed to support risk reduction measures and recovery options. Availability Management works collaboratively with this process on the assessment of business impact and risk, and the provision of resilience, failover, and recovery mechanisms.

> 📋 ***Cross-Reference:*** *Infrastructure availability and backup requirements are governed by Sections 4.9.3 and 4.9.4.*

2.5.13 Service Design

The Contractor **MUST** design products and services that are fit for purpose, fit for use, and deliverable by the organization and its ecosystem. The Contractor **MUST** work with OHIP Technology leadership and stakeholders, including business managers, service managers, and technical architects, to ensure that all design activities are consistent and aligned with the overall business strategy.

All design activities **MUST** be documented, controlled, and monitored to ensure compliance with required standards and delivery within specified timelines. This includes ensuring a holistic design approach considering all four ITIL dimensions, coordinating design activities across projects, producing System Architecture Design Documents (SADDs), and managing the IT service portfolio. The IT service portfolio is revisited in anticipation of major changes to OHIP's strategy or transformation programs.

2.5.14 Service Desk

The Contractor **MUST** capture demand for incident resolution and service requests. The service desk **MUST** be the entry point and single point of contact for the Contractor with all its users.

2.5.14.1 Service Desk Overview

The Service Desk practice provides a clear path for users to report issues and request services, acting as the single point of contact between Contractor and users. The Contractor **MUST** establish a Service Desk for intake and triaging of service requests related to the IT solution implemented and supported. The Contractor **MUST** be responsible for the communication and transition of service requests to the OHIP’s Service Desk for solutions or services that they do not provide support.

2.5.14.2 Multi-Tiered Support Model

OHIP operates a multi-tiered support model (L0 through L4) aligned with industry standards and vendor engagement patterns. Tier definitions are provided in Appendix D: ITIL 4 Framework Reference.

Tier Transition Requirements

Transitions between support tiers **MUST** follow established handoff procedures to ensure continuity and avoid information loss. When transitioning from L0 to L1, automated ticket creation captures self-service attempt history so that L1 staff understand what the user has already tried. Transitions from L1 to L2 require ticket updates documenting the troubleshooting performed and results observed. Escalation from L2 to L3 requires ticket updates with technical analysis and vendor engagement per contract requirements. When L3 vendors engage L4 upstream support, OHIP **MUST** be informed, and external ticket references **MUST** be cross-referenced in the OHIP ticket record.

2.5.15 Service Desk Integration

The Contractor **MUST** coordinate with:

- OHIP Business Support functions for L0 integration
- Contact Center operations
- Other vendor service desks for cross-solution issues

Support triage, assignment, and escalation **MUST** be seamless across all tiers with clear SLAs and hand-off procedures.

Suggested KPIs for these practices (Service Desk Management) are provided in Appendix F, Table 42.

2.5.16 Service Level Management

The Contractor **MUST** meet the clear business-based targets for service levels, and to ensure that delivery of services is properly assessed, monitored, and managed against these targets. This includes negotiating and agreeing on SLAs, monitoring and reporting on service performance, conducting service reviews, and identifying and implementing improvements based on performance.

SLAs and LD (LDs) are defined through the procurement processes and incorporated into vendor contracts. The Contractor and OHIP Technology leadership **MUST** engage in initial negotiations on the SLAs and LDs, and when making periodic adjustments. The Contractor **MUST** be responsible for reporting on the SLAs for the components and service management processes related to their solution.

2.5.17 Service Request Management

The Contractor **MUST** support the agreed quality of a service by handling all pre-defined, user-initiated service requests in an effective and user-friendly manner. This includes defining and publishing available service requests, providing clear fulfillment workflows, automating fulfillment where possible, and communicating status to manage user expectations.

The Contractor **MUST** triage and accept or transfer back each service request. Requests **MUST** be evaluated and, if approved, implemented using the change enablement process as described in the Contractor's M&O Plan. The Contractor **MUST** emphasize self-service capabilities where appropriate.

Suggested KPIs for these practices (Service Request Management) are provided in Appendix F, Table 43.

2.5.18 Service Validation and Testing

The Contractor **MUST** ensure that new or changed products and services meet defined requirements and specifications before being deployed.[13] This includes defining and managing test plans, cases, and scripts; conducting functional, performance, and usability testing; and validating that services will deliver the expected value.

> 📋 ***Cross-Reference:*** *Test planning and management (test plans, cases, and scripts, and the conduct of functional, performance, and usability testing) are governed by the Solution Delivery Domain Document, Test Management Standard (Section 6.0). This section addresses the ITIL service validation and testing practice and does not redefine those test management requirements.*

Post-implementation evaluation is required for releases of new functionality or changes to existing functionality. The Contractor **MUST** perform post-implementation testing of all changes to verify that functionality is performing as expected and that security boundaries have not been modified as a result of the change. Each Change Request **MUST** be updated by the Contractor in OHIP's solution to verify that post-implementation testing has been successfully completed.

Suggested KPIs for these practices (Service Validation and Testing) are provided in Appendix F, Table 44.

2.6 Technical Management Practices

This section describes technical management practices focused on managing technological components and integrating with modern development approaches.

2.6.1 Deployment Management

The Contractor **MUST** follow standards to move new or changed hardware, software, documentation, processes, or any other component to live environments, including deployment planning and scheduling, executing deployments across environments, providing early life support post-deployment, and managing deployment automation and Continuous Integration/Continuous Delivery (CI/CD) pipelines.

The Contractor **MUST**:

- Execute deployment activities, including deployment planning, scheduling, execution, and providing early life support; and ensure staff perform the actual transfer, deployment, and retirement of system functionality under the direction of the Release and Deployment Manager.
- Provide deployment runbooks and rollback procedures to OHIP, and develop, manage, and publish a formal and documented procedure to ensure the integrity of the release package.
- Support the Transition-Out phase, where the Contractor transitions its activities to OHIP or a Successor Contractor; acknowledge that this phase **MAY** occur during or at the end of the Contract Term; and recognize that the scope areas include System Architecture, Project Management, M&O, and Design, Development, and Implementation (DDI).
- Begin Transition-Out activities only after OHIP approves the initiation of the Transition-Out phase.

---

[13] For more information, refer to the OHIP Solution Delivery Domain Document, Test Management Standard.

- Ensure any transition is performed in a way that provides OHIP with uninterrupted services of its solutions, including performing a complete and total transfer of all data, files, reports, and records generated from the inception through the end of the Contract to OHIP or a Successor Contractor.
- Provide technical and business process support as necessary and required by OHIP to transition Contract requirements to OHIP or a Successor Contractor.
- Develop a Transition-Out Schedule to identify and manage all Transition-Out activities and tasks required by the Transition-Out Plan, and to securely and smoothly transfer data and records generated from the inception through the end of the Contract.

2.6.2 Infrastructure and Platform Management

The Contractor **MUST** oversee the infrastructure and platforms they provide, enabling the monitoring and management of technology products and services. This includes managing servers, networks, storage, and directory services; managing middleware, databases, and application platforms; monitoring infrastructure and platform health; and coordinating with suppliers of infrastructure components.

The Contractor **MUST** provide guidance and leadership of the technical management functions related to their solution, including server management, network management, application (batch, Managed File Transfer [MFT]), middleware, and database administration. This includes all daily operational activities needed to manage IT Operations according to the performance standards defined by OHIP.

2.6.3 Solution Development and Management

The Contractor **MUST** ensure that applications meet internal and external stakeholder needs in terms of functionality, reliability, maintainability, compliance, and auditability. This includes managing SDLCs (Agile, Waterfall, or Hybrid;[14] integrating development with service management (Change, Release, Deployment); ensuring code quality,[15] testing, and compliance; and managing development backlogs and priorities.

The Contractor **MUST** follow OHIP SDLC Standard and integrate with CI/CD pipelines as appropriate. Code quality standards, testing requirements, and security scanning (static and dynamic) **MUST** be met before any production release.[16]

[14] For more information, refer to the OHIP Solution Delivery Domain Document, SDLC Standard.
[15] For more information, refer to the OHIP Solution Delivery Domain Document, Code Standard.
[16] For more information, refer to the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard.

2.7 Management Roles, Responsibilities, and Tools

This section describes the high-level roles, responsibilities, and tools used to manage IT services supplied by the Contractor. The Contractor **MUST** fill these roles with qualified staff, and depending on contract size and complexity, roles **MAY** be combined with OHIP approval.

2.7.1 System Manager Role

The System's Manager is responsible for technology capacity, availability, and performance management for the solution, including proactive monitoring, capacity planning, continual improvement initiatives, and coordination with OHIP stakeholders. This role **SHOULD** perform the following minimum responsibilities:

- Provide technology capacity, availability, and performance management.
- Measure, monitor, and manage application performance optimization, availability, uptime, and runtime improvements.
- Identify and manage appropriate system capacity for all components of their solution, including production and non-production environments.
- Identify performance, capacity, and business drivers, understanding the impact to the program, and developing solutions.
- Follow an agreed upon schedule for developing models, utilizing tools, and developing solutions that proactively avoid any disruption or degradation of service.
- Ensure the appropriate system capacity and performance is delivered.
- Draft requirements for planning, managing, and reporting system capacity in coordination with OHIP Business and OHIP Technology leadership.
- Develop a System Capacity Plan which details the requirements for planning, managing, and reporting system capacity.
- Comply with the Contract requirements for a maximum response time, maximum processing time for each request, and minimum number of requests that can be processed in each period.
- Leverage industry standard tools for the monitoring, analysis, and tuning of capacity and performance.
- Forecast future capacity needs based on industry standard practices.
- Monitor, measure, analyze, and report availability.
- Ensure their solution’s availability and reliability is compliant with an agreed-upon set of requirements.
- Develop availability reports to document and maintain all availability and performance analysis results.
- Develop demand estimates for their solution in coordination with OHIP Business and OHIP Technology leadership.

2.7.2 Service Desk Roles

A first-line analyst role (L1) **MUST** provide a first point-of-contact support by taking calls and handling incidents or service requests.

- The goal is to resolve [80% TBC] of the calls placed to the service desk upon first contact.

- The initial level of support (L0) **MUST** be able to handle 75% TBC of calls without escalation.
- Escalation to second tier support (L2) or to other services desks **MUST** be seamless.
- Roles include first-line analysts providing initial point-of-contact support, Service Desk Manager supervising operations, and coordination roles ensuring integration with OHIP Business Support and other vendor service desks.

2.7.3 Maintenance and Operations (M&O) Roles

The M&O-related practice manager roles are listed below:

- The Incident Manager is expected to represent the first stage of escalation for incidents, **SHOULD** these not be resolvable within the agreed service levels.
- The Event Manager is responsible for the Event Management Practice and is responsible for managing the practice to detect events.
- The Problem Manager is responsible for the Problem Management Practice and is responsible for prevention of Incidents from reoccurring, and to minimizing the impact of Incidents that cannot be prevented.
- The Continual Improvement Manager (formerly Continuous System Improvement [CSI] Manager) is responsible for measuring the performance of the Contractor and design improvements to processes, services, and infrastructure to increase efficiency, quality, and cost effectiveness.
- The Service Desk Manager is expected to supervise the processes and activities associated with the service desk, including output management, console operations, and production control.

2.7.4 Change Enablement Supporting Roles

The Contractor **MUST** fill the following roles with the staff on their contract:

- The Change Manager is responsible for change implementation coordination. This role carries out triage, assessment, prioritization, risk categorization, and closure of change records. The Change Manager is technically responsible for change control activities and is required to support the OHIP project governance activities related to change control.
- The Change Member is expected to contribute to change record review, change authorizations, and validating impact and resources assessments. This group **MUST** include people with a clear understanding of the whole range of stakeholder needs.
- The Risk Evaluation Manager is responsible for identifying, assessing, and controlling risks to the solution or services.
- The Configuration/Asset Manager is responsible for service asset and configuration management. This role carries out the configuration management and planning activities and interfaces with support teams, business, and project resources. This role **SHOULD** be responsible for performing periodic audits of the CMDB to ensure accuracy and reliability of data as defined by the OHIP.

2.7.5 Release and Deployment Management Roles

The Release and Deployment Manager is expected to perform the following minimum responsibilities within their role:

- Aspects of the end-to-end release processes, promoting releases through the development and initial test environment, as well as the production environment.
- Producing formal documentation of all build notes for all releases including emergency releases.
- Submitting release documentation, including build notes, test results/certificate to OHIP for acceptance of the release.
- Communication with OHIP, including pre- and post-notifications if the deployment involves downtime.

Deployment Staff are expected to perform the following minimum responsibilities within their role:

- Performing deployment planning and preparation, as well as performing the actual transfer, deployment, and retirement of system functionality.
- Development, management, and publishing of a formal and documented procedure to ensure the integrity of the release package.

Early Life Support Staff are expected to perform the following minimum responsibilities within their role:

- Monitoring the quality of recently deployed changes, service enhancements, and/or additional releases of functionality.
- Verifying the adherence to release criteria and successful deployment to the appropriate environment(s).

2.7.6 Application and Technical Management Roles

The Applications Manager is responsible for the guidance and leadership of the applications management function, which includes application (e.g., batch and MFT), middleware, and database administration.

The Infrastructure Manager is responsible for the guidance and leadership of the technical management function that includes, but is not limited to, server management, network management, and directory services.

2.7.7 IT Operations Management Function Roles

The IT Operations Manager is responsible for the IT Production Control/Operations. This role is also responsible for the daily operational activities needed to manage the IT Operations according to the performance standards defined by OHIP.

The Second-Line Analysts are advanced support entities, who take over incidents/service requests that are not able to be solved immediately with the means of First-Line Analyst. This role tends to focus on deeper rooted, technical incidents. Role(s) that the Contractor **MUST** staff that fall into the category of Second-Lines Analysts include: Process Analyst, IT Engineer / Systems Monitoring Analyst, Batch Monitoring Analyst, Programmer Analyst, Production Control Analyst, Infrastructure Architect, Service-Oriented Architecture [SOA] Architect, Application Architect, Technical Solution Architect, Database Architect, IT Service Continuity Analyst, and Service Architect.

2.8 ITSM Tools and Technology

The Contractor **MUST** leverage industry-standard tools providing the following required capabilities. The focus is on the required functionality and interoperability, not a specific software, unless part of OHIP's standardization strategy.[17]

Service Management Core Capabilities:

- Incident tracking and management
- Service request fulfillment
- Problem management and known error database
- Change enablement and approval workflows
- Release and deployment management
- Asset and configuration management (CMDB)
- Knowledge management and self-service portals

Integration and Interoperability:

- API-based integrations with other ITSM tools
- Data synchronization capabilities
- Workflow orchestration across systems
- Reporting and analytics consolidation

The Contractor MAY use their existing ITSM tools provided they:

- Meet all capability requirements above
- Support integration with OHIP enterprise tools
- Provide required reporting and metrics
- Support transition to future enterprise tooling per the defined strategy

The Contractor **SHOULD** maintain compatibility with tools identified in the OHIP Preferred Operational Tools Standard, participate in tool standardization initiatives, support data migration to enterprise tools when required, and provide tool training and knowledge transfer.

OHIP is working toward an Enterprise Service Catalog (see Section 2.5.10) and having a Centralized ITSM tool as system of record.

2.9 Vendor and Partner Integration

OHIP operates in a multi-vendor environment where effective integration and coordination across multiple Contractors is essential for delivering seamless IT services. This section outlines the framework for integrating ITSM processes across vendors, partners, and OHIP Technology Leadership.

[17] For more information regarding OHIP's approved enterprise-wide tools, refer to Section 8.0.

2.9.1 Integration Principles

The Contractor **MUST** adhere to the following integration principles:

- Seamless service delivery across vendor boundaries
- Transparent hand-offs and escalations between support tiers
- Coordinated incident and problem management across systems
- Unified reporting and performance measurement
- Consistent change management and deployment coordination

2.9.2 OHIP and Contractor Responsibilities

The Contractor **MUST** align operational roles with the ITIL role framework defined in Appendix D: ITIL 4 Framework Reference.

The Contractor **MUST** map their internal roles to the OHIP and State Enterprise role framework described above. Named individuals **MUST** be designated for each required role, and role assignments **MUST** be provided to OHIP during contract onboarding. Any changes to personnel in these roles **MUST** be communicated to OHIP within five business days. For systems classified as Critical, the Contractor **MUST** ensure 24/7 coverage for the Incident Manager role.

The Contractor **MUST** coordinate with the State for infrastructure-level services and with other OHIP vendors for cross-solution issues. Clear escalation paths and integration procedures will be established to ensure effective collaboration.

2.9.3 Integration with OHIP's ITSM Solution

OHIP maintains an ITSM platform for coordinating service management activities across vendors and systems. The capabilities represented below are the required implementations as identified by OHIP Technology Leadership. Each capability will be detailed with specific requirements, acceptance criteria, and integration specifications during the implementation phase.

- **Incident Management**: Enables development and IT operations teams to respond to, resolve, and continuously learn from incidents.
- **Problem Management**: Group incidents to problems, fast-track root cause analysis, and record workarounds to minimize the impact of incidents.

The Contractor **MUST** support integration with OHIP's ITSM Solution as specified in individual contracts and integration agreements.

Continuous Service Management Integration

The Department is committed to the continuous improvement of its ITSM capabilities. Future enhancements will be implemented iteratively to broaden the scope of services managed within OHIP's ITSM solution, including the progressive rollout of advanced capabilities in:

- Request Management
- Change Management
- Asset Management

- Configuration Management
- Knowledge Management

Project and Configuration Standards

The standards governing configuration ensure consistency in how incidents, problems, and service requests are managed across the OHIP ecosystem. Refer to the list below for reference:

- **Project Structure**: Projects are organized by system and vendor domain to maintain clear boundaries of responsibility while enabling cross-project visibility where needed. Current OHIP projects include OHIP Enrollment and Eligibility (E&E). Medicaid Eligibility and Client Management System (MECM), and Maximus, with additional projects established as new systems are onboarded to the platform. The creation of new projects requires approval from OHIP Technology Leadership and **MUST** follow established naming conventions and configuration templates to ensure consistency across the enterprise.
- **Priority Focus Areas**: Initial implementation focuses on Incident Management and Problem Management as the foundational practices for cross-vendor coordination. Incident Management brings development and IT operations teams together to rapidly respond to, resolve, and continuously learn from incidents affecting OHIP systems. Problem Management enables grouping of incidents to problems, fast-tracking root cause analysis, and recording workarounds to minimize the impact of recurring incidents.
- **User Access**: User Access Management represents a future phase capability that will standardize User Access Requests and User Access Reviews across vendors once the foundational incident and problem management processes are mature. Expansion to additional practices including Change Management, Release Management, and Asset Management will be evaluated following successful Phase 1 implementation based on organizational readiness and business priorities.
- **Cross-System Ticket Dependency Management**: When an OHIP incident is dependent on or related to a ticket in a non-integrated external system such as ITS ServiceNow or a vendor-specific platform, specific protocols **MUST** be followed to ensure proper tracking and resolution coordination. Because these external systems are not integrated with OHIP through automated synchronization, manual cross-referencing and communication are required to maintain visibility across system boundaries.
- **Documentation Requirements**: The Contractor **MUST** record external ticket references in the designated custom field. The external reference **MUST** include the External System Name, External Ticket ID, External Ticket Status, and the Contact Name for the external ticket owner. All communications with external system contacts **MUST** be maintained within ticket comments to create a complete audit trail.
- **Status Management**: When an OHIP ticket is blocked by an external dependency, the ticket status **MUST** be updated to Pending External Resolution. Follow-up reminders **MUST** be set at intervals appropriate to incident priority. All status updates received from the external system **MUST** be documented in the ticket to maintain an accurate record of resolution progress.
- **Escalation Protocol**: If an external ticket shows no progress within defined timeframes, escalation to the OHIP System Manager is required. For Priority 1 incidents, escalation is required if no progress is observed within two (2) hours. For Priority 2 incidents, the threshold is four (4) hours. For Priority 3 incidents, escalation is required after one (1) business day without

progress. The OHIP System Manager coordinates with the external system owner to align priorities and ensure appropriate attention is given to the dependency.

- **Resolution Requirements**: An OHIP ticket cannot be closed until the external dependency is resolved or an acceptable workaround is implemented and documented. Final ticket documentation **MUST** include a summary of the external ticket resolution, and any lessons learned that **MAY** inform future cross-system coordination.

Integration Standards

The Contractor operating external ITSM platforms **MUST** establish integration with OHIP's ITSM solution using one of the approved integration patterns. API Integration provides real-time bidirectional synchronization and is the preferred approach when technically feasible. Webhook Integration enables event-driven notifications for systems that support this capability. As such, Scheduled Synchronization provides batch data exchange at defined intervals for systems where real-time integration is not practical. Manual Cross-Reference is permitted for systems without integration capability but requires a documented process for maintaining ticket references and communication.

Integration specifications, authentication requirements, and data mapping **MUST** be defined in individual vendor integration agreements.[18] The Contractor is responsible for maintaining their integration in accordance with these specifications and notifying OHIP of any changes that **MAY** affect cross-system visibility.

Reference Integration Models

OHIP maintains documentation of successful integration patterns that **MAY** serve as reference architectures for new vendor integrations. The Contractor implementing new integrations **MUST** consult with OHIP Technology Leadership regarding applicable reference models and lessons learned from previous implementations.

2.9.4 Vendor-to-Vendor Coordination

OHIP's multi-vendor environment requires standardized coordination procedures to ensure seamless service delivery across system boundaries. When incidents, problems, or changes span multiple OHIP systems or involve multiple Contractors, clear protocols **MUST** govern how vendors communicate, coordinate resolution activities, and maintain accountability for outcomes.

Cross-Solution Issue Management

- **Lead Vendor Designation**: When an incident or problem spans multiple OHIP systems or vendors, the vendor whose system first exhibited symptoms or received the initial report serves as the Lead Vendor. The Lead Vendor is responsible for overall incident coordination until resolution or until a formal handoff occurs. The OHIP System Manager **MAY** reassign Lead Vendor designation based on root cause determination if investigation reveals that another vendor's system is the primary source of the issue.
- **Communication Requirements**: The Lead Vendor establishes the primary communication channel, typically through a ticket with conference bridge as needed for higher priority incidents. All involved vendors **MUST** respond within escalation timeframes defined in their respective

[18] For more information on authentication and integration, refer to the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard.

SLAs. Status updates **MUST** be posted to the shared ticket at intervals appropriate to the incident priority level.

- **Ticket Linking**: All related vendor tickets **MUST** be linked in OHIP's ITSM solution using standard link types to maintain visibility across the incident life cycle. Each vendor maintains their own ticket while referencing the master incident record maintained by the Lead Vendor. This approach ensures that each vendor can track their specific activities while OHIP maintains a consolidated view of the overall incident.

Cross-System Ticket Dependencies

Where incidents or service requests span multiple vendor ITSM systems that are not integrated through automated synchronization, the following requirements apply:

- Manual synchronization is required between systems when API integration is not available.
- The Lead Vendor is responsible for maintaining the master ticket record and ensuring all relevant information is captured.
- Related ticket references **MUST** be documented in each system to enable cross-referencing.
- Updates **MUST** be communicated within agreed timeframes to ensure all parties have current information about incident status and resolution progress.

Escalation Procedures

The Contractor **MUST** establish escalation paths that enable timely resolution of incidents at each support tier. Escalation from L1 to L2 occurs when initial troubleshooting is unable to resolve the issue and technical expertise beyond L1 capability is required. Escalation from L2 to L3 occurs when the issue requires vendor-specific expertise or access to code and configuration that only the Contractor can address. Escalation to executive management is triggered when incidents exceed resolution timeframes or when cross-vendor conflicts cannot be resolved at the technical level.

Specific escalation timeframes are defined in individual vendor contracts and SLAs. The Contractor **MUST** ensure their internal escalation processes support achievement of contracted service levels. When cross-vendor coordination is required, all involved vendors share accountability for the combined response and resolution time, with individual contributions tracked separately for performance reporting.

Conflict Resolution

When vendors disagree on responsibility for an issue, resolution follows an established escalation path. Initial resolution is first attempted through vendor technical leads and the OHIP System Manager. If the conflict remains unresolved, it is escalated through the appropriate OHIP channels for mediation and recommendations. OHIP Leadership makes the final determination and communicates the decision to all appropriate stakeholders. In the event the conflict persists after leadership determination, a final resolution is provided by the Contract Manager.

Conflicts **MUST** be resolved expeditiously to avoid impact to service delivery. For Priority 1 and Priority 2 incidents, resolution of vendor responsibility disputes **MUST NOT** delay active incident response activities. Vendors are expected to continue collaborative troubleshooting while responsibility determination is in progress.

2.9.5 Escalation Procedures

Effective escalation procedures are essential to ensuring that incidents receive appropriate attention and resources throughout the resolution life cycle. This section establishes protocols for escalating incidents within and across organizational boundaries, with particular emphasis on major incident response.

Major Incident Conference Bridge Protocol

For Priority 1 and Priority 2 incidents affecting critical systems, the Contractor **MUST** establish or participate in conference bridges to enable real-time coordination of response activities. These protocols ensure that all necessary parties are engaged promptly and that communication flows effectively throughout the incident life cycle.

- **Conference Bridge Activation**: For Priority 1 incidents, the responsible Contractor **MUST** establish or join a conference bridge within fifteen minutes of incident declaration. For Priority 2 incidents, a conference bridge **MUST** be established within thirty minutes if the incident affects multiple systems or requires cross-vendor coordination. When a conference bridge already exists for a related issue, the Contractor **MUST** join the existing bridge rather than establishing a separate call. Bridge consolidation decisions rest with the OHIP Incident Coordinator.
- **Required Participants**: Conference bridges for major incidents **MUST** include the Contractor Incident Manager or designated technical lead as a required participant. The OHIP System Manager or designated delegate **MUST** also participate. Subject Matter Experts (SMEs) are engaged as needed based on the technical nature of the incident. Additional vendors are included when cross-system impact is identified. The Contractor hosting the bridge is responsible for ensuring bridge information is shared with the OHIP Incident Coordinator immediately upon establishment.
- **Communication Cadence**: During active Priority 1 incidents, status updates **MUST** be provided at minimum every thirty (30) minutes. For Priority 2 incidents, status updates are required at minimum every sixty (60) minutes. All updates **MUST** be posted to the ticket and communicated via established channels to ensure that stakeholders not participating in the conference bridge receive timely information.
- **Escalation Triggers**: If an incident is not contained within one (1) hour of bridge activation, escalation to include OHIP Technology Leadership is required. If a resolution path is not identified within two (2) hours for Priority 1 incidents or four hours for Priority 2 incidents, escalation to vendor management is required. The OHIP Incident Coordinator is responsible for determining when additional escalation is warranted based on incident trajectory and impact.

3.0 Application Integration Standard

3.1 Introduction

The Application Integration Standard establishes the mandatory requirements for how OHIP MES solutions exchange data with each other, with federal and state systems, and with external partners. In a modular MES environment where eligibility, claims, provider management, pharmacy, and data warehouse systems operate as independent modules connected through shared interfaces, integration failures can cascade across the enterprise leading to a disruption of beneficiary services, compromising federal reporting, and exposing sensitive Medicaid data.

This standard governs all integration methods, including but not limited to RESTful and FHIR APIs, X12 EDI transactions, event-driven messaging, and file transfers; and requires every integration to be routed through OHIP-approved gateways and brokers. It mandates compliance with national data exchange standards (HL7, FHIR R4, ASC X12N), enforces centralized API governance and discoverability, and establishes resilience requirements to ensure that no single interface failure results in data loss or service disruption. The OHIP Secure API Development Baseline, maintained under the OHIP Security, Privacy, and Compliance Domain, is a companion standard that governs the security and privacy dimensions of API development; this standard governs the architectural, interoperability, and operational dimensions.

Compliance with this standard is required for CMS SMC and for OHIP's sustained eligibility for enhanced FFP. Associated deliverables and artifacts are located in Appendix A.

3.2 Objectives

The primary objectives of this Standard are to:

- Centralize API management through a required API Gateway to enforce security, routing, and monitoring policies consistently.
- Mandate compliance with national data exchange standards, such as HL7 FHIR and X12 EDI, to ensure interoperability.
- Promote the adoption of resilient EDA for real-time data exchange and system decoupling.
- Ensure all integrations are observable and reliable through comprehensive logging, monitoring, and error-handling requirements.

3.3 Integration Governance

The Contractor **MUST** comply with the following integration governance requirements for compliance review, Hypertext Transfer Protocol Secure (HTTPS) usage; and API publishing, policy enforcement, and registry and ownership:

- **Integration Compliance Review:** Ensure that proposed integrations conform to this standard and the relevant federal/industry standards before implementation by submitting integration plans and designs to OHIP for review and approval.
- **HTTPS Inbound:** All inbound interfaces for a new OHIP system **MUST** utilize HTTPS.

> 📝 ***Note:*** *This HTTPS Inbound requirement applies to APIs and to all new inbound interfaces and interactions for an OHIP solution. For example, newly created bulk or large file inbound data transfers* ***MUST*** *utilize HTTPS. Terminal access to new cloud systems* ***MUST*** *use native cloud services over*

*HTTPS. Exceptions **MUST** be granted by OHIP for any protocol other than HTTPS (e.g., File Transfer Protocol Secure [FTPS], Secure File Transfer Protocol [SFTP], and Secure Copy Protocol [SCP]) used for newly created inbound interfaces for an OHIP system.*

- **API Gateway**: All exposed APIs **MUST** be published through an OHIP-approved API gateway, which **MUST** serve as the single-entry point that enforces policies (routing, throttling, authentication, inspection, encryption, service metadata, and monitoring) for all API traffic.[19]

📝 ***Note:** If a Contractor cannot use OHIP's preferred API gateway, the Contractor **MUST** provide an explanation for OHIP to approve. To be approved by OHIP, an alternate API Gateway **MUST** provide governance of APIs. The governance **MUST** include API life cycle management, including monitoring, securing, and documenting. The API gateway **MUST** comply with the resiliency and performance requirements of the project.*

- **Policy Enforcement:** The API gateway **MUST** enforce authentication for both end-user and service-to-service calls, applying consistent security controls across all integrations.
- **Registry and Ownership:** All integration interfaces (APIs, message feeds, and file transfer endpoints) **MUST** be registered in a catalog with designated owners. Each interface entry **MUST** include version, contact, and performance information as well as availability SLAs and usage policies for governance and life cycle management. All new interfaces are documented and modeled in OHIP's Enterprise Architecture tool.[20]

Before creating new interfaces, the Contractor **MUST** first search OHIP registries to identify opportunities to re-use existing services/interfaces (making any necessary modifications).

3.4 Integration Compliance, Patterns, and Interoperability

3.4.1 Adoption of Industry Standards

The Contractor **MUST** use nationally recognized data exchange standards per CMS requirements[21] in all integrations. This includes compliance with the HIPAA-adopted transaction standards (e.g., ASC X12N EDI)[22] under the Affordable Care Act's (ACA), CMS's,[23] and relevant Office of the National Coordinator for Health IT's (ONC) interoperability standards as follows:

- **HL7 Messaging:** Where clinical or public health data is exchanged, the Contractor's implemented solutions **MUST** support the latest release version consistent with maintaining interoperability of HL7 messaging for events, such as admissions, lab results, orders, and immunizations. Messages **MUST** follow the HL7 v2 (or later) defined profiles for structure and content.

---

[19] For more information, refer to NIST SP 800-228.
[20] For more information, refer to the OHIP Data and Information Domain Document, Data Architecture and Naming Standard.
[21] For more information, refer to Enhanced Funding Requirements: Seven Conditions, Industry Standards Condition.
[22] For more information, refer to the Transactions Overview at CMS.gov.
[23] For more information, refer to the CMS Standards and Implementation Guide.

- **FHIR APIs:** All new application integrations exposing health data implement HL7 FHIR R4 (or later) for RESTful APIs. APIs implemented by the Contractor **MUST** use standard FHIR resources and profiles (e.g., US Core) to maximize interoperability.
- **X12 EDI Transactions:** Medicaid administrative data exchanges (e.g., claims, eligibility, enrollment, and prior auth) use Accredited Standards Committee (ASC) X12N or later EDI formats as mandated by HIPAA. All required Medicaid transactions **MUST** adhere to the X12 Implementation Guides for content and code sets.
- **General Web and RESTful API Standards:** For integrations that do not fall under nationally recognized healthcare data exchange standards (e.g., HL7, FHIR, X12), APIs implemented by the Contractor **MUST** conform to organization-approved web and interoperability standards to ensure consistent, reusable, and governed information exchange across systems.

All such APIs **MUST**:

- Implement RESTful design principles and publish interface definitions using Open API specifications for documentation and discovery.[24]
- Exchange data using structured, machine-readable formats such as JSON with defined schemas or data models approved by OHIP.
- Non-standard or proprietary interfaces are not allowed unless an exception is approved and documented.

3.4.2 Event-Driven and Asynchronous Integration Patterns

The Contractor **MUST** comply with the following event-driven and asynchronous integration requirements:

- **EDA Adoption**: For scenarios requiring real-time updates, high scalability, and loose coupling between systems, the Contractor's implementations **MUST** utilize asynchronous EDA. EDA patterns **MUST** provide loose coupling so that a producing system can publish events without direct dependencies on the availability of consuming systems. Each consuming system is responsible for reacting to events in accordance with its own processing and availability requirements.
    - Event-driven patterns used **SHOULD** utilize standard protocols (e.g., Advanced Message Queuing Protocol [AMQP] 1.0, JMS, or MQTT) and standardized frameworks for event payload structure and metadata (e.g., CloudEvents[25]).
    - All event topics, queues, and subscriptions **MUST** be registered in an OHIP-approved event catalog with defined ownership, description, and data contracts.
- **Standardization of Event Structures and Taxonomies**: all events published within or consumed by OHIP solutions adhere to OHIP-approved standardized event structures, including common headers, metadata, and data schemas.
    - A central event catalog and taxonomy **MUST** be maintained for discoverability, reuse, and consistent event interpretation.

[24] For more information, refer to OpenAPI Specification - Version 3.1.0 | Swagger.
[25] For more information, refer to GitHub - cloudevents/spec: CloudEvents Specification.

    - Schema evolution policies **MUST** be enforced to ensure backward and forward compatibility and to prevent breaking changes for downstream consumers.

- **Push-Pull Mechanisms and Webhooks:** Push-based event notification mechanisms (e.g., webhooks) are used where immediate change notification is required. Pull mechanisms (e.g., scheduled API polling) are permitted only where push-based notification is impractical.
    - Approved Use Cases and integration patterns **MUST** be documented and reviewed for both push-based mechanisms and pull-based mechanisms for consistency across the enterprise.
- **Data Streaming and Real-time Processing:** dedicated streaming platforms are utilized for integrations involving continuous, high-volume data flows (e.g., telemetry, log aggregation, and real-time analytics).
    - Architecture and integration patterns **MUST** ensure efficient ingestion, processing, and distribution of data while maintaining scalability and fault tolerance.
    - Data streams **MUST** be monitored and support retention and replay capabilities to enable recovery and auditing.
    - Schemas for data streams **MUST** be versioned and managed to ensure backward and forward compatibility. A centralized schema registry **MUST** be used to enforce schema evolution policies.

3.4.3 Integration Protocol Minimum Requirements

The Contractor **MUST** adhere to the minimum requirements for integration methods:

Table 5 – Integration Methods Minimum Requirements

Integration Method	Minimum Requirements
API (RESTful and FHIR)	• Comply with the security controls specified in NIST SP 800-228 “Guidelines for API Protection for Cloud-Native Systems”.[26] • Use JSON (or Extensible Markup Language [XML] payloads) conforming to FHIR resource schemas for health data. • Support RESTful operations (GET/POST/PUT, etc.) and use consistent Uniform Resource Identifier (URI) structures. • Use an OHIP-approved API Gateway for governance.
EDI Transactions (X12)	• Use ASC X12N standard transactions for HIPAA-covered exchanges. • Use HTTPS for inbound EDI. • Transmit via secure channels (e.g., AS2 over HTTPS or outbound SFTP [no plain FTP]). • Ensure acknowledgment and response mechanisms are in place for EDI exchanges.

[26] For more information, refer to NIST SP 800-228.

Outbound File Transfers[27]	• Use secure protocols (e.g., HTTPS, SCP, SFTP or FTPS) for file transfers. • Use encryption for all files, which contain sensitive data, in transit and at rest. • All files sent or received **MUST** be automatically scanned for viruses, malware, and signature prior to transmission and upon receipt. Any file that fails inspection **MUST** be quarantined (or blocked) automatically, an alert sent to the Security and Privacy, and all scan results logged to Security Incident Event Management (SIEM). Threat definitions **MUST** be updated at least daily to ensure up-to-date protection. • All secure file transfers **MUST** be managed via an OHIP-approved solution. • For any batch file exchange, the receiving system **SHOULD** return an acknowledgement to the sending system confirming receipt and processing outcome (e.g., accepted, accepted with errors, rejected). An exception **MAY** be granted through the Standards Deviation Request process (Section 1.7.1) where the batch file is a one-way distribution and non-transactional.
Event-Driven Messaging	• Integrations **MUST** employ, publish/subscribe, or message queue patterns for real-time data distribution (e.g., HL7 v2 ADT feeds and event streams). • Event messages **MUST** be no larger than 256KB. Larger messages **MUST** utilize API. • Use a messaging broker or event bus supporting reliable delivery (with acknowledgments and durable queues). • Design event messages to be idempotent[28] and include timestamps/IDs to prevent duplicate processing. • Events and event messages **MUST** travel through an OHIP-approved event broker or message broker.

3.5 Integration Quality and Monitoring

The Contractor **MUST** comply with the following integration quality and monitoring requirements:

- **Logging and Audit Trails:** All integrations **MUST** produce detailed logs, which are accessible by OHIP, for auditing and troubleshooting. Every transaction, message transfer (successes and failures), and source of IP address with timestamps, source/destination, and outcome **MUST** be logged.

[27] Inbound Batch file transfers require an OHIP exception for newly developed inbound integrations.
[28] For more information, refer to JSON Server, Idempotency.

    - Logging **SHOULD** follow the Open Web Application Security Project's (OWASP's) logging cheat sheet.[29] All logs **SHOULD** be accessible for potential analysis with an OHIP-approved analysis tool.[30]

- **Monitoring and Alerts:** Projects **MUST** implement continuous monitoring of integration workflows by tracking key metrics (e.g., throughput, latency, and error rates) for APIs, message queues, and file transfers. The Contractor **MUST** set up automated alerts for failures, anomalous activities, or SLA breaches (e.g., API downtime), so issues are addressed promptly, and **MUST** automatically create incidents as agreed to by the Department. Incidents created from integration failures **MUST** be managed per Section 2.5.5.
- **Data Validation:** Integration endpoints **MUST** validate data content and format against schemas or implementation guides. For example, HL7 messages **MUST** be checked against HL7 profile specifications (ensuring required segments/fields are present), and FHIR API responses **MUST** conform to the FHIR schemas. Invalid or non-conforming messages **MUST** be rejected with error notifications.

📝 ***Cross-Reference:*** *Enterprise log management requirements, including event categories, log field specifications, sensitive data restrictions, and retention periods, are governed by Section 5.0. Integration-specific logging requirements in this section supplement, and do not replace, the enterprise log management requirements.*

📝 ***Cross-Reference:*** *Enterprise data quality and data validation requirements, including data quality gates and thresholds, are governed by the Data and Information Management Domain Document (Data Quality, Sections 2.15 and 7.6). The integration-layer schema and message-format validation in this section supplements those data quality requirements.*

3.6 Integration Change Control

All integration changes are subject to the change enablement process defined in Section 2.5.4. This section defines additional requirements specific to integration interfaces.

The Contractor **MUST** comply with the following integration change control requirements:

- **Version Control**: Backward-incompatible changes to an existing version of integration interfaces are not allowed unless an exception is approved and documented.
    - Changes to an API or message format require a new version (e.g., v2 API or new HL7 messaging version) rather than breaking existing Contracts[31] to allow transition.
- **Change Approval:** Proposed changes to integrations (e.g., new API endpoints, schema changes, and partner connectivity changes) **MUST** go through a formal change control process. Changes **MUST** be documented (e.g., what is changing and why) and approved by OHIP before implementation. In the event of an Emergency Change, a retrospective review is required.

---

[29] Refer to OWASP Logging Cheat Sheet: Logging - OWASP Cheat Sheet Series.
[30] Refer to Section 5.0.
[31] In this context, a deprecation period is the time frame where all interface users have been notified the version is available and usable, but the version will be removed and made unavailable at a given date. Users must transition to a newer approved implementation or stop using the interface before the duration ends.

- **Impact Analysis:** Every integration change request **MUST** include an impact analysis, including affected systems, data impacted, and compliance review. In this assessment, the requestor **MUST** validate that changes will not violate standards or security. For example, adding a new data field **MUST** still comply with HIPAA privacy rules and CMS standards.
- **Partner Coordination:** Changes **MUST** be coordinated with all stakeholders. If an interface is consumed by external partners or other agencies, those parties **MUST** be notified well in advance of changes. The Contractor **MUST** provide testing opportunities to adapt to new versions. The Contractor **MUST** obtain OHIP approval for all testing opportunities and their corresponding results prior to production deployment.
- **Documentation Updates:** Integration documentation and catalogs **MUST** be updated as part of the change rollout. Any interface version change **MUST** include updating API specifications and interface control documents (ICD), and publishing release notes for consumers.

3.7 Integration Test and Validation

The Contractor **MUST** comply with the following integration test and validation requirements:

- **Standards Compliance Testing:** All integrations **MUST** be validated for compliance with relevant standards during development and prior to Go-Live. For example, HL7 and FHIR interfaces **MUST** be tested with HL7/FHIR validators, and X12 EDI files **MUST** be tested with syntax checkers.
- **Test Endpoints:** A test (non-production) set of endpoints **MUST** be made available for integration testing by external applications. The test endpoints **MUST** be able to:
    - Provide the same robust security mechanisms and validations as production.
    - Access a secure non-production environment.
    - Provide secure data stores (to prevent accidental data exfiltration due to external non-OHIP testers accidentally testing with live data).
    - “Reset” data.
    - Mirror production APIs, including versioning consistency.
    - Provide realistic data and scenarios.
    - Provide additional, specific test endpoint documentation and developer documentation.
    - Utilize only test credentials.

> 📝 ***Cross-Reference:*** *Integration testing supplements the enterprise testing governance established by the Solution Delivery Domain Document, Test Management Standard (Section 6.0). The standards-compliance, validator, and test-endpoint requirements in this section apply in addition to those enterprise testing requirements and do not replace them.*

3.8 Error Handling and Resilience

The Contractor **MUST** comply with the following error handling and resilience requirements:

- **Graceful Error Handling:** Integrations **MUST** handle errors gracefully without data loss. Any error or exception in an integration flow **MUST** trigger appropriate logging and notifications. Any error messages returned to users or partners **MUST** be sanitized and informative (e.g., “Invalid

data format") without revealing sensitive internal details. Internal logs **MUST** capture the technical details for troubleshooting.

- **Retry and Recovery:** The Contractor **MUST** implement retry mechanisms for transient failures. For example, if an API call to a partner system fails or a message delivery to a queue is not acknowledged, the system **MUST** retry after a suitable interval. Retries **MUST** be bounded with back-off[32] to avoid infinite loops.
- **Idempotency**: The Contractor **MUST** design integrations to be idempotent,[33] so that retrying does not create duplicate transactions.
- **Resilience Patterns**: Resilience techniques such as load balancing and circuit breakers **MUST** be used to avoid single points of failure. For instance, if a downstream service is unresponsive, a circuit breaker **MUST** stop repeated calls and trigger fallback logic, such as queuing messages for later processing.
- **Failover and Continuity**: Critical integration components **MUST** have high-availability and failover plans. For message queues and integration platform runtimes, implement clustering or backups so if one node fails, messages are not lost, and processing continues on another node. For file transfers, ensure files are not lost if a transfer is interrupted. The Contractor **SHOULD** implement checkpoint/restart mechanisms and verify file integrity upon transfer completion.
- **Error Notification**: The Contractor **SHOULD** establish automated alerts for integration errors. When errors occur (e.g., a failed message or authentication error), responsible support teams **SHOULD** be notified (via email/SMS/Dashboard) in real time. Backout queues or dead-letter queues **SHOULD** be monitored daily, and all unresolved errors **SHOULD** be tracked to closure via an incident management process.

3.9 Documentation and Discoverability

The Contractor **MUST** comply with the following documentation and discoverability requirements:

- **Interface Specifications**: All integration interfaces **MUST** have comprehensive documentation. This includes API specifications (e.g., OpenAPI/Swagger definitions), data models, sample requests/responses, message schema definitions, and EDI companion guides, as applicable. Documentation **MUST** be kept up to date with the latest version of the interface and readily accessible to developers and partners.
- **Central API Catalog**: API definitions (for discovery) **MUST** be hosted in a format accessible to client developers.
    - Each integration entry in the catalog **MUST** include metadata tags (e.g., data domain, owning team, and compliance category, such as "HIPAA PHI") to facilitate search and governance. Consumers **MUST** be able to find APIs or data feeds relevant to their needs through the catalog without needing insider knowledge.
- **Developer Support**: To promote proper usage, the Contractor **MUST** provide test endpoints and example clients for APIs. Documentation **MUST** include any authorization requirements and a sample credential setup (without exposing secrets). A support contact or forum for integration

[32] Backoff is a strategy used to manage the rate of retries by gradually increasing the delay between retries after each failure.
[33] For more information, refer to JSON Server, Idempotency.

consumers **MUST** be indicated in the documentation for issue resolution and onboarding assistance. The Contractor **MUST** escalate interoperability issues and risks to OHIP for facilitation and resolution.

- **Document Maintenance:** Documentation **MUST** be treated as a required deliverable for any new integration or change. As part of deployment, teams **MUST** update relevant documents and catalog entries. Incomplete or outdated documentation is not acceptable. Integration points are considered incomplete until documentation and discoverability requirements are met in full.

> 📝 ***Cross-Reference:*** *The Integration Technical Design Document (ITDD) and ICD are governed by the Solution Delivery Domain Document (requirements SDLC-0167 and SDLC-0168). The requirements in this section govern the operational publication, cataloging, discoverability, and maintenance of integration documentation and do not redefine those design deliverables.*

4.0 Infrastructure Management Standard

4.1 Introduction

The Infrastructure Management Standard establishes the mandatory requirements for provisioning, governing, and operating cloud infrastructure services that host OHIP MES solutions. As OHIP transitions to a cloud-first delivery model with SaaS as the preferred approach, Contractors **MUST** operate within a governance framework that addresses security, cost management, performance, automation, and compliance across all cloud service models.

This standard defines the shared responsibility model between OHIP, Cloud Service Providers, and Contractors for SaaS, PaaS, and IaaS implementations. It establishes requirements for standardized environments (development through Disaster Recovery (DR) [DR]), operational controls for change management, storage, backup, and availability, and performance monitoring and reporting obligations. All infrastructure decisions, architectural designs, and cloud service selections require OHIP review and approval.

Compliance with this standard is required for CMS SMC and for OHIP's sustained eligibility for enhanced FFP. Associated deliverables and artifacts are located in Appendix A.

4.2 Objectives

The primary objectives of this Standard are to:

- Provide a framework that guides the adoption, implementation, and management of infrastructure services across the Department's cloud environments in alignment with CMS requirements.
- Prioritize a cloud-hosted delivery model, with SaaS as the preferred model for all new solutions.
- Establish clear governance and responsibilities across different cloud service models[34] (SaaS, PaaS, IaaS).
- Require standardized, isolated environments for development, testing, and production to ensure a stable and secure lifecycle.
- Define monitoring and reporting mechanisms for infrastructure environments, promoting continuous improvement and optimization.

4.3 OHIP Infrastructure Management Strategy

The Contractor **MUST** adhere to the following requirements regarding IT solutions for the Office of Health Information Programs (OHIP):

- Implement a cloud-hosted delivery model, with SaaS as the preferred service model.
- Host Enterprise Cloud Solutions on a cloud infrastructure maintained by personnel located in the continental United States.

---

[34] Service delivery models include Platform as a Service (PaaS), Software as a Service (SaaS) [34], Infrastructure as a Service (IaaS).

- Ensure the solution resides in a cloud environment that complies with the latest federal security requirements, such as FedRAMP Moderate or higher, ARC-AMPE, and Social Security Administration (SSA) requirements, in addition to any other OHIP-specific requirements related to SaaS, PaaS, IaaS offerings, and/or architecture.
- Utilize the security framework outlined in the OHIP Security and Privacy Compliance Standard for the provisioning of necessary security requirements for infrastructure and managed services.
- Submit exception requests for review and approval by OHIP.

While SaaS is the preferred model, the Contractor **MUST** provide support for other service models as needed, following the standards outlined for PaaS and IaaS implementations. All cloud environment ownership used for the solution **MUST** belong to OHIP.

4.4 Infrastructure Landscape and Governance Scope

4.4.1 Infrastructure Services and Solution Models

The Contractor **MUST** provide infrastructure solutions using OHIP-approved cloud service models (SaaS, PaaS, or IaaS). SaaS is the preferred model. The Contractor **MUST** recommend specific PaaS types based on solution requirements for OHIP evaluation and approval. Cloud service model definitions are provided in Appendix B: Requirements Summary.

4.4.2 Roles in Providing Infrastructure Services

OHIP has identified the key roles in Table 6 that facilitate informed decision-making on OHIP's enterprise infrastructure.

Table 6 – OHIP Enterprise Infrastructure Key Roles

Key Role	Description
OHIP	OHIP consists of various teams collectively responsible for ensuring that the IT solutions provided by the Contractor are optimal for the business and adhere to all State and federal regulations.
Cloud Service Provider (Contracted Cloud Vendor)	The Cloud Service Provider provides hosting and infrastructure for solutions hosted in physical and cloud data centers. It is a third-party company that provides scalable computing resources through their platforms that businesses can access on demand over a network, including cloud-based computing, storage, platform, and application services.
The Contractor	The Contractor is an external organization that develops and manages solutions for OHIP. It collaborates with OHIP's IT team to ensure seamless integration, customization, and ongoing maintenance of its solution. The Contractor also adheres to established governance standards, complies with relevant regulations, and commits to specified performance metrics and SLAs.

4.5 OHIP and Provider Partner Roles and Responsibilities

4.5.1 Infrastructure Management Functions and Responsibilities

Figure 1 introduces the key infrastructure management functions that the Contractor **MUST** perform when delivering services and solutions.

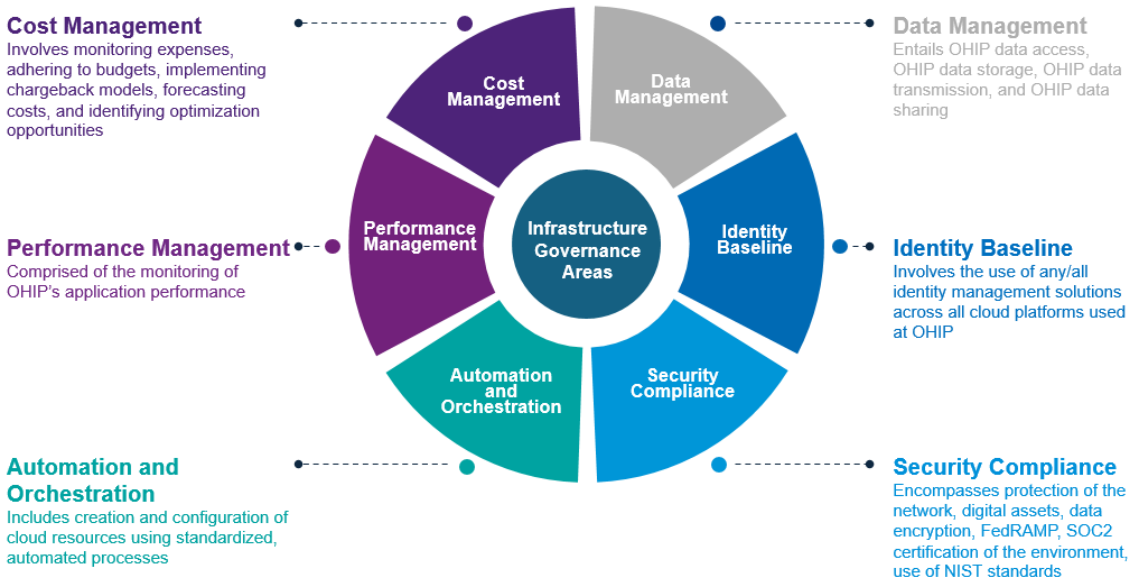


Figure 1: Infrastructure Management – Standard Structure

4.5.2 Infrastructure Management Functions

The Infrastructure Management Functions cover key aspects of cloud service governance, including security and privacy compliance, cost management, data management, infrastructure automation and orchestration, identity baseline, and performance management. The governance responsibilities of OHIP, the Cloud Service Provider, and the Contractor across each service model (SaaS and P/IaaS) are defined in Appendix D.

The Contractor **MUST** provide detailed infrastructure documentation and specifications for OHIP to assess service levels and security measures, identify areas for improvement, and evaluate potential risks in cloud services. The governance requirements for each function are detailed in Sections 4.5.2.1 and 4.5.2.2 below.

4.5.2.1 Software as a Service (SaaS) Governance

SaaS governance refers to the policies, guidelines, and processes established by OHIP to effectively manage and govern the adoption, usage, and ongoing operation of SaaS services. It ensures that SaaS services align with OHIP's strategic goals, comply with regulations and security requirements, and deliver value while minimizing risks.

Cost Management

The Contractor **MUST**:

- Provide OHIP with the usage/cost of each cloud component broken down by account/subscriptions or as required by the Contract with the Contractor.
- Perform analytics on usage of the cloud environment over periodic intervals (e.g., time series) and make this information available to OHIP.

- Comply with all requirements of the OHIP Infrastructure and Operations Domain Document, Cloud FinOps Standard.

Security and Privacy Compliance[35]

The Contractor **MUST** comply with all requirements of the OHIP Security and Privacy Compliance Standard, including requirements for hosting, data loss protection tools, threat protection activities, and reporting security vulnerabilities.

Data Management

The Contractor **MUST**:

- Collaborate with OHIP to seek necessary approvals for proper data usage, isolation, and separation.
- Maintain audit logs of access to OHIP's data and support OHIP in audits required by federal and state agencies.
- Comply with OHIP data governance policies, standards and procedures.
- Provide data management practices, including but not limited to, data isolation, separation, and usage for OHIP review, approval, and auditing.

Infrastructure Automation and Orchestration

The Contractor **MUST**:

- Review and seek approval of the infrastructure architecture through the OHIP review process.
- Maintain a Bill of Materials for the cloud services and software the solution uses and provide details to OHIP.
- Adhere to all standards, procedures, and/or policies concerning the use and integration of OHIP Enterprise monitoring tools.

The Contractor **MUST** also obtain OHIP review and approval, at minimum, for the following:

- Infrastructure architecture before building the solution.
- All cloud services and software used in the solution.
- Any major and/or significant changes to the infrastructure or architecture before use and/or production usage.

Performance Management

The Contractor **MUST** collaborate with OHIP to develop and maintain the SLAs. SLA dashboards **MAY** be created to monitor adherence to SLAs as agreed upon in the Contract.

The Contractor **MUST** submit all SLAs to OHIP for review and approval before execution.

> 📋 ***Cross-Reference:*** *Detailed Cloud FinOps requirements including cost allocation, tagging, and reporting are governed by Section 7.0.*

[35] Refer to the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard.

4.5.2.2 Platform/Infrastructure as a Service (P/IaaS) Governance

All SaaS governance requirements defined in Section 4.5.2.1, including Cost Management, Security and Privacy Compliance, Data Management, and Performance Management, apply equally to PaaS and IaaS implementations. The following additional requirements apply to P/IaaS:

Cost Management

In addition to complying with Section 7.0, the Contractor **MUST** obtain OHIP review and approval for:

- All costs incurred for storage, computing, and other cloud resources used in the solution.

Infrastructure Automation and Orchestration

In addition to the SaaS infrastructure automation requirements in Section 4.5.2.1, the Contractor **MUST**:

- Submit a Cloud Design Document (CDD) or SADD, or equivalent, as part of the OHIP architecture review process and receive approval before implementation.
- Implement infrastructure automation and orchestration through containerization and CI/CD pipelines.
- Work with OHIP to reduce legacy solution footprints.
- Obtain OHIP review and approval, at minimum, for:
    - Architecture, design, and implementation of all infrastructure components.
    - Containerization implementation and the CI/CD pipeline for each Release.

> 📋 ***Cross-Reference:*** *Detailed Cloud FinOps requirements including cost allocation, tagging, and reporting are governed by Section 7.0.*

4.6 Operational Governance Standards

The standards in this section apply across SaaS, PaaS, and IaaS solutions. Where a requirement is specific to a particular service model, this is noted. The Contractor **MUST** apply these standards in the context of the solution and service model deployed.

The Contractor **SHOULD**:

- A monthly budget for each application, broken down by cloud component.

4.6.1 Enterprise Standards

4.6.1.1 Environments

All solutions, whether SaaS, PaaS, or IaaS, **MUST** go through traditional solution life cycles; however, there are several unique considerations for cloud-based solutions. OHIP has an existing OHIP SDLC standard that applies. The standards below are intended to be complementary and specific to cloud-based considerations.

The Contractor **MUST** provide the necessary environments to develop and test changes to the solution by following the OHIP Solution Delivery Domain Document, SDLC Standard. Enterprise applications, including Business systems, IT systems, application development, or any customized solutions, **MUST** include the following minimum environments: Development (DEV), Data Conversion, TEST/ System Integration Testing (SIT), User Acceptance Testing (UAT)/Stage, Performance, Pre-Production (PRE-

PROD), Production (PROD), and DR.[36] Additional environments, such as Sandbox (SBX) or Training, **MAY** also be required based on project needs and approval from OHIP. Any exceptions from the following environments require explicit approval from OHIP Leadership.

All environments are required, unless stated otherwise in the table below. The Contractor **MUST** comply with the following requirements[37] for each environment:

Table 7 – Infrastructure Management Environments

Environment and Purpose	Key Requirements of the Environment
Development (DEV) For development use and unit testing of software	• Use synthetic data only; no CII/PHI/PII permitted • Have stable code and not impact other application components or providers. Non-stable code **MUST** be tested in the Sandbox Environment • **MUST NOT** impact other providers during deployments
Test / SIT For demonstration if a program, function, or integrated system component complies with requirements and objectives as stated in the requirements specification	• Use synthetic or masked data only; no CII/PHI/PII permitted • Intended primarily for the Contractor's lower environment testing and validation, which includes regression testing • Made available to other module providers
UAT / Stage For testing conducted by the user or consumer to determine whether a system satisfies the defined user acceptance criteria in an isolated environment	• Use synthetic or masked data; no CII/PHI/PII permitted • Coordinate with OHIP to determine UAT environment name • Report system changes and maintenance to Contractor and OHIP stakeholders • Adhere to the OHIP Program and Project Management Domain Document, Technical Change Control Standard for infrastructure/platform changes; adhere to the OHIP Program and Project Management Domain Document, Project Change Control Standard for scope/baseline changes.
Performance For verification that the performance of a system complies with service-level agreements and	• Use synthetic or masked data only; no CII/PHI/PII permitted • Provide OHIP with performance testing results prior to go-live

[36] Only the Production and Disaster Recovery (DR) environments may have production data. All other environments must have Synthetic data with no Client Confidential Information (CCI), Personally Identifiable Information (PII), or Protected Health Information (PHI).
[37] For more information, refer to the OHIP Solution Delivery Domain Document, Test Management Standard, Requirements Management Standard, and Release Management Standard.

measures the behavior of the system with increasing load.	• System **MUST** meet required SLA levels before go-live or Release
Pre-Production (PRE-PROD) Used for implementing or testing a solution for an issue identified in the Production environment	• **MUST NOT** contain sensitive data. Mirror the Production environment cluster, which includes: the hardware, software, middleware, data and various internal/external connectivity • Once the solution successfully resolves the issue identified in PRE-PROD, it **MUST** be applied in the DEV environment and then propagated to the PROD environment. • Adhere to the OHIP Program and Project Management Domain Document, Technical Change Control Standard for infrastructure/platform changes; adhere to the OHIP Program and Project Management Domain Document, Project Change Control Standard for scope/baseline changes.
Production (PROD) Concerns the live environment where software products and applications are used by end-users in real-world scenarios	• Certified to hold production data, including PII/PHI • Adhere to the OHIP Program and Project Management Domain Document, Technical Change Control Standard for infrastructure/platform changes; adhere to the OHIP Program and Project Management Domain Document, Project Change Control Standard for scope/baseline changes.
DR The environment necessary for DR testing or in the event of a disaster	• Certified to hold production data including PII/PHI • Meet SLA availability requirements • Full failover testing is conducted initially, annually, or as required by OHIP • Adhere to the OHIP Program and Project Management Domain Document, Technical Change Control Standard for infrastructure/platform changes; adhere to the OHIP Program and Project Management Domain Document, Project Change Control Standard for scope/baseline changes.
SBX *(Conditional, as required by OHIP)* Intended use is to run and analyze the code in a safe, isolated environment without affecting the application, system, or Platform.	• Use synthetic data only; no CII/PII/PHI • Used for patching, upgrades, proof-of-concept pilots, and bug identification
Training *(Conditional, as required by OHIP)*	• Only use synthetic data

Custom data for use to support training activities	

4.6.1.2 Business Continuity and Disaster Recovery (BC/DR) Plan

The Contractor **MUST** address BC/DR responsibilities for OHIP production environments as follows:

- Document a comprehensive BC/DR Plan for all production solutions, for approval by OHIP.
- Perform a successful DR Test for any new solution before going live, with results documented and provided to OHIP.
- Conduct an annual DR Test, providing the documented results to OHIP.
- Submit a comprehensive report of DR test results within two weeks of the test, addressing all issues until OHIP approves passing results.
- Ensure production changes supporting BC/DR (e.g., multi-AZ, failover, DR runbooks) are deployed using the OHIP Solution Delivery Domain Document, Release Management Standard and approved via the OHIP Program and Project Management Domain Document, Technical Change Control Standard.
- Submit BC/DR architecture and test evidence as part of the OHIP architecture review and approval process.

4.7 Technology Standards

The Contractor **MUST** adhere to technology standards when proposing or procuring cloud technologies for OHIP:

- Refer to Section 8.0 and understand OHIP-approved shared services before making proposals or procurements.
- Formally request and obtain approval from OHIP for any modifications to the technology used for OHIP solutions.
- Obtain approval from OHIP before installing or implementing any software.
- All approvals for technology changes **MUST** be executed through the OHIP Program and Project Management Domain Document, Technical Change Control Standard; this section defines what requires approval, not the approval workflow.

4.8 Operational Standards

The Contractor **MUST**:

- Provide OHIP with complete visibility with appropriate access to OHIP-owned cloud resources through a portal.
- Provide administrative access and observability (performance dashboard, health monitoring, admin console) necessary to operate OHIP-owned cloud resources; incident/change workflows remain governed by Section 2.0 and the OHIP Program and Project Management Domain Document, Technical Change Control Standards.
- Track and report on their applications' performance and manage performance issues for any Contractor-managed solution that supports OHIP.

- Define and document the ownership of each cloud component's support accountabilities, responsibilities, and processes collectively.
- The Contractor **MUST** leverage native cloud services where applicable and approved by OHIP. The Contractor **MUST** document any vendor lock-in risks associated with native cloud service adoption and present alternatives to OHIP for evaluation.

4.9 Operational Controls

The Contractor **SHOULD**:

- Maintain all solutions at an 'n-1' version level.

4.9.1 Change Control

The Contractor **MUST** adhere to the following change control requirements:

- Follow the OHIP Program and Project Management Domain Document, Technical Change Control Standard for all infrastructure/platform changes (cloud resources, network, compute, storage, CI/CD infrastructure, identity configurations, monitoring integrations).
- Follow the OHIP Program and Project Management Domain Document, Project Change Control Standard only for changes to scope, schedule baseline, funding, or contractual deliverables.
- No change to production or controlled environments **MAY** proceed without an approved change record in the OHIP change tracking solution.
- Log change requests prior to implementation and meet lead-time requirements defined by OHIP Program and Project Management Domain Document, Technical Change Control Standard (or contract, if stricter).
- For changes with cross-solution impact, include documented impact analysis and evidence of required architecture review approvals.
- Patches/upgrades **MUST** follow an approved Patch Management Plan[38]; schedules **MUST** be submitted to OHIP and executed through the OHIP Program and Project Management Domain Document, Technical Change Control process.

📝 ***Cross-Reference:*** *ITSM-level change enablement processes are governed by Section 2.5.4.*

4.9.2 Storage Management

The Contractor **MUST** adhere to the following storage management requirements for OHIP solutions:

- Ensure regular reporting on storage utilization includes total storage usage, types of storage (e.g., fiber, glacial), burn rates or growth trends, and forecasted storage needs for future periods.
- Provide storage forecasts at a frequency determined by OHIP, considering factors such as growth rate, budgeting and reporting periods, and data gathering needs. The reporting frequency **MUST NOT** exceed annually.

[38] For more information regarding the Patch Management Plan deliverable, refer to the OHIP Solution Delivery Domain Document, Code Standard.

The Contractor **SHOULD**:

- Document and report all storage usage to OHIP monthly, including details of current storage utilization, hosting entities, and any storage eligible for release.

4.9.3 Availability and Recoverability

The Contractor **MUST** adhere to the following availability and recoverability requirements for OHIP's cloud solutions:

- Build all core infrastructure to provide a minimum of four 9's (99.99%) availability, with scalability designed to accommodate higher tiers of application hosting in the cloud environment.
- Ensure that availability requirements for infrastructure-based solutions are specified within individual contracts and SLAs, with these contractual SLAs taking precedence if not covered by the standard availability requirements.
- Design cloud solutions to meet agreed-upon availability requirements, utilizing innate cloud redundancy features, such as availability zones, to exceed traditional primary and backup data center approaches.
- Leverage local redundancy for data as a minimum standard and implement geo-redundancy (e.g., through availability regions) as necessary to fulfill availability and recoverability requirements.

4.9.4 Backup Management

The Contractor **MUST** adhere to the following backup management requirements for OHIP solutions:

- Perform daily full backups and weekly full database backups as outlined in the contract, including daily incremental (partial) backups as a minimum standard for all environments.
- Provide evidence of backup completion and frequency to OHIP, investigate and re-run any failed backups daily to ensure no daily full backups are skipped or missed.
- Retain backups per OHIP records retention, contract requirements, and approved backup retention schedules (minimums defined by applicable OHIP retention standards).[39]
- Document, review, and obtain OHIP approval for the backup schedule, frequency, and retention policy for all cloud-based solutions.
- Regularly validate the backups, incorporating backup recovery and testing as part of the backup management process.
- Ensure solutions automatically perform backups on a configurable frequency, providing redundancy that meets or exceeds requirements.
- Enable creation of application, infrastructure, and environmental backups, archiving data in accordance with Department policies and contractual requirements.
- Ensure all backups and redundancy copies conform to data residency requirements to avoid legal or regulatory conflicts with OHIP and federal requirements.

---

[39] For more information, refer to Section 5.0.

4.10 Monitoring and Optimization Standards

The Contractor **MUST**:

- Comply with all OHIP policies and ensure cloud-based solutions are interoperable with existing OHIP toolsets, alerting processes, and monitoring expectations.
- Use evolving cloud service capabilities to support enhanced active monitoring, optimization, visibility, and continuous improvement.
- Identify all servers under management and maintain complete, accurate host details in the OHIP CMDB as the authoritative source of truth (in alignment with OHIP's ITSM Service Configuration Management).
- Log OHIP-required demand requests for adding or removing servers.
- Ensure PaaS and IaaS solutions can produce raw, unredacted vulnerability, compliance, code-scan, and penetration-test results in formats shareable with OHIP.
- Proactively identify cost-saving opportunities, including new cloud technologies, pricing models, and discounts.
- Provide a configurable, comprehensive, and OHIP-interoperable alerting mechanism for monitoring infrastructure, applications, and services.
- Provide analytical and operational reporting capabilities, such as log analytics, that interoperate with the OHIP Enterprise Solution. Log retention and retention periods are governed by Section 5.0.
- Provide OHIP with access to operational and usage statistics upon request.
- Monitor, track, and report on all infrastructure components, including network, storage, compute, services, and applications, providing itemized cost allocations as needed.
- Design cloud-solution controls that optimize chargeable components, minimize data-egress costs, and effectively manage licenses.
- Design and build cloud-based solutions using current resilience-leading practices to protect against DDoS, spoofing, man-in-the-middle, and other physical and cyber threats.

4.11 Incident and Event Management

The Contractor **MUST** adhere to the following incident and event management requirements for OHIP:

- Track all incidents and events comprehensively.
- Report any solution outages as incidents in OHIP's tracking solution.
- Ensure that all OHIP solutions are monitored using enterprise monitoring tools, with events reported directly to OHIP's logging tool.
- Ensure enterprise monitoring integrations can automatically generate incident records in OHIP's ITSM tooling where required.
- Ensure cloud solutions are interoperable with OHIP enterprise tools, including File Integrity Monitoring (FIM), Security Operations Center (SOC), and Security Incident Event Management (SIEM).

> 📝 ***Cross-Reference:*** *Incident management processes, escalation procedures, and SLA requirements are governed by Section 2.5.5.*

4.12 Performance Standards

The Contractor **MUST** adhere to the following performance standards for OHIP solutions:

- Monitor, scale, document, and report performance metrics in accordance with OHIP standards.
- Ensure adherence to performance metrics is maintained to guarantee a positive end-user experience and optimal response times.
- Measure solution performance using OHIP's five categories: User Interface (UI), Application Response Time, Real-Time Interfaces, Data Queries, and Image Response Time.
- Provide specifics on calculation methods and minimum SLAs in each procurement.

4.13 Operational Performance Measurement and Reporting

The Contractor **MUST** adhere to the following operational performance measurement and reporting requirements for OHIP:

- Capture the elements necessary to measure performance for all specified performance standards, ensuring compliance with the minimum data elements required for SLA performance reporting are defined in Appendix C.
- Report performance measurements to OHIP at least monthly, or according to the frequency agreed upon with OHIP.
- Include performance measurements for the following categories: UI, Application Response Time, Real-Time Interface, Data Queries, and Image Response Time.

4.14 Operational Performance Monitoring

The Contractor **MUST**:

- Ensure all solutions, whether cloud-based or on-premises, are continuously monitored.
- Implement ongoing performance management that includes collaborative performance baselining.
- Conduct performance monitoring and reporting, including alerts and other necessary notifications.
- Establish processes for detecting and resolving performance degradation, utilizing autoscaling where applicable.
- Engage in continuous performance improvement practices.
- Scan inbound and outbound data traffic for reputation, malware, spam, and other criteria defined by OHIP.

5.0 Log Management Standard

5.1 Introduction

The Log Management Standard establishes the mandatory requirements for generating, collecting, protecting, retaining, and analyzing log data across all OHIP MES solutions. In a Medicaid environment that processes PHI, PII, and FTI, comprehensive logging is not optional; it is a regulatory obligation and an essential control for detecting unauthorized access, investigating security incidents, and maintaining program integrity.

This standard defines the specific audit events that must be logged (authentication, privileged access, data access, business transactions, and configuration changes), the mandatory fields for each event category, and the characteristics that all logs must exhibit (immutability, timestamping, completeness). It establishes restrictions on logging sensitive data, defines retention periods aligned with federal and state requirements, and requires integration with OHIP's enterprise log analysis tools.

Compliance with this standard is required for CMS SMC and for OHIP's sustained eligibility for enhanced FFP. Detailed citations for OHIP MES logging requirements are provided in Appendix E.

5.2 Objectives

The primary objectives of this Standard are to:

- Ensure regulatory and policy compliance by aligning logging practices with applicable federal, State, and OHIP requirements, including the State Archive Standards.[40]
- Create a consistent and unified approach to log management, including the retention and monitoring of logs for all stakeholders operating within the OHIP MES ecosystem.
- Enable the timely detection, investigation, and analysis of security events, anomalies, and potential data breaches by creating a comprehensive and reliable audit trail.
- Establish uniform requirements to ensure all system activities are traceable, thereby protecting sensitive data and ensuring the integrity of all program transactions.
- Provide trustworthy log data to support program integrity audits, compliance reporting, risk management activities, and other oversight functions.

5.3 OHIP Logging Governance

The Contractor **MUST** support OHIP in the timely identification, search, retrieval, analysis, and presentation of log data related to MES operations when required, to respond to audits, investigations, oversight inquiries, public record requests, litigation, or other legal or regulatory matters. This support includes providing complete and unaltered log records, relevant metadata, documentation of logging configurations, and subject matter expertise necessary to interpret the records. The Contractor **MUST** preserve log integrity, maintain chain-of-custody where applicable, and ensure that requested information is provided within the timeframe specified by OHIP, consistent with applicable security, privacy and confidentiality requirements.

[40] For more information, refer to NYS Archives - Retention Schedules.

> 📝 ***Cross-Reference:*** *Integration-specific logging requirements, including API transaction logging and OWASP compliance, are governed by Section 3.5. Infrastructure-level monitoring and event logging are governed by Section 4.10. This section establishes the enterprise log management framework that supplements both.*

5.3.1 Audit Events Record Generation and Content Requirements

In compliance with the related publications: (National Institute of Standards and Technology [NIST] SP 800-53 AU 02), (CMS ARC-AMPE Volume I), (NYS-S14-005), and (HIPAA 164.312[b]), the Contractor **MUST** ensure that all OHIP MES solutions generate logs for security-relevant and business-critical events, minimally including, but not limited to:

- **Authentication Success/Failure:** The Contractor **MUST** ensure that all attempts for authentication success/failure are recorded to verify the identity of a user or system when accessing MES resources. This includes log-ins, logouts, and any validation of credentials or tokens used to establish a session. The record content **MUST** minimally include the Log Fields defined in Appendix E, Table 24 – Authentication Success/Failure Log Fields
- **Privileged Access:** The Contractor **SHOULD** ensure that all activities performed by users or system accounts with elevated permissions that allow them to administer, configure, or override standard system controls are recorded. This includes any use of administrative roles or capabilities that could significantly impact system behavior, security, or data integrity. The record content **SHOULD** minimally include the Log Fields defined in Appendix E,
- Table 25 – Privileged Access Log Fields.

> 📝 ***Note:*** *The Contractor **MUST NOT** use generic Admin accounts for Privileged Access. Rather, the Contractor **MUST** assign a specific account to a particular user and grant the account Admin privileges via role-based access.*

- **Data Access (PHI/PII/FTI):** The Contractor **MUST** ensure that all interactions with sensitive data, particularly PHI, PII, and FTI are recorded. This includes when such data is viewed, created, modified, deleted, or extracted, enabling traceability of who accessed sensitive information and for what purpose. The record content **MUST** minimally include in the Log Fields defined in Appendix E,
- Table 26 – Data Access (PHI/PII/FTI) Log Fields.

> 📝 ***Note:*** *The Contractor **MUST** ensure the Data Access logging mechanisms support both security monitoring and compliance with the HIPAA Privacy Rule, including the ability to identify and document, where required, certain disclosures of PHI pursuant to (45 CFR 164.528)[41] and (45 CFR 164.524)[42].*

- **Business Transactions:** The Contractor **MUST** ensure that all record business-level actions that create, modify, or finalize Medicaid program data are logged. This includes operational transactions such as claims processing, eligibility determinations, enrollments, and provider

[41] 45 CFR 164.528
[42] 45 CFR 164.524

updates, ensuring that all changes to program records are traceable and auditable. The record content **MUST** minimally include the include the Log Fields defined in Appendix E, Table 27 – Transactions Log Fields.

- **Configuration Changes:** The Contractor **MUST** record any modifications to system settings, application behavior, infrastructure components, or security configurations. These events capture changes that could affect how the system operates, how data is processed, or how access is controlled, providing accountability for system alterations. The record content **MUST** minimally include the include the Log Fields defined in Appendix E, Table 28 – Configuration Changes Log Fields.

The Contractor **MUST** also include the following common log fields and adhere to the requirements in Appendix E,

Table 29 – Cross-Cutting Log Fields

5.3.2 Log Characteristics Requirements

The Contractor **MUST** ensure that:

- Access and changes to Medicaid data are logged and traceable.[43]
- MES components synchronize system clocks to a common authoritative time source for the origin of log events.
- Logs are:
  - Forwarded to the OHIP SIEM centralized logging solution for aggregation and correlation.
  - Protected against unauthorized access, modification or deletion.
  - Actively monitored and reviewed.
  - Retained in accordance with federal, NYS, and OHIP regulations and Medicaid Program requirements.
- Logs support:
  - Filtering, querying, and reporting capabilities.
  - Traceability of events back to individual systems.
  - Integration by feeding incident response tools and audit reporting systems.

📝 ***Cross-Reference:*** *SIEM integration requirements for infrastructure solutions are also addressed in Section 4.11.*

5.4 Sensitive Data Log Restrictions

The Contractor **MUST NOT** log sensitive data without the explicit direction from OHIP. Sensitive data includes any information for which loss, misuse, unauthorized access, or alteration could negatively impact the national interest, the operation of federal programs, or the privacy rights guaranteed under 5

[43] See Appendix A: Deliverables and Artifacts

U.S.C. § 552a (the Privacy Act of 1974). Logs **MUST NOT** contain sensitive data or data with special protections under New York law unless specifically directed by OHIP. If OHIP directs specific sensitive data to be logged, such logs **MUST** be protected with measures equal to those applied to the protection of the sensitive data itself.[44]

The following sensitive data categories are subject to this restriction:

- **PHI**: Individually identifiable health information as defined under HIPAA (45 CFR §160.103)
- **Individually Identifiable Health Information**: A subset of health information created or received by a covered entity that identifies or could identify an individual (45 CFR §160.103)
- **PII**: Information that can be used to distinguish or trace an individual's identity, as defined by NIST SP 800-122 and ITS-P22-001
- **FTI**: Federal tax returns and return information governed by IRS Publication 1075 and 26 U.S.C. § 6103
- **SSA Supplied Data**: Data provided under the SSA/State Data Exchange, subject to SSA matching requirements.[45]
- **MCD**: Information subject to safeguards under §1902(a)(7) of the Social Security Act (42 United States Code [USC] §1396a(a)(7)) and 42 CFR §431.300

Detailed definitions for each sensitive data category are provided in Appendix G: Standard Terminology. The Contractor **MUST** implement log sanitization controls, including data masking, tokenization, or hashing, to prevent any of the above data types from appearing in log output unless explicitly authorized by OHIP.

5.5 Retention Periods

The Contractor **MUST** adhere to the log file retention times specified in Table 8. If a log file **MUST** be retained beyond its designated retention period due to containing relevant, helpful information for future reference, it is the responsibility of the Contractor to work with OHIP to ensure that these specific logs are moved to an OHIP-designated location before the destruction of the log (after it has reached its maximum retention time). If a log file contains multiple types of data with different retention periods, the longest retention period **MUST** be used.

Table 8 – Log Retention Periods

Log or Data Type	Retention Period	Policy Statement	Regulation
Audit Logs of FTI	Minimum of seven (7) years	The Contractor **MUST** retain audit records of FTI for the required period of seven (7) years	To be compliant with IRS Pub 1075 9.3.3.4 Audit Storage Capacity (AU-4)
Logs tracking the location of FTI data	Minimum of five (5) years	The Contractor **MUST** maintain a tracking system to identify and track the location of electronic and non-electronic FTI from	To be compliant with IRS Pub 1075 3.2

[44] For more information, refer to the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard.
[45] SSA-provided data can be included in FTI and PII data.

Log or Data Type	Retention Period	Policy Statement	Regulation
		receipt until destruction. These records **MUST** be maintained for five (5) years.	Electronic and Non- Non-Electronic FTI Logs
Audit Logs of Electronic PHI (ePHI)	Minimum of six (6) Years from the date of its creation or the date when it last was in effect, whichever is later	The Contractor **MUST** retain audit logs for at least six (6) years if logging information related to actions on systems containing ePHI.	To be compliant with HIPAA and NIST SP800-66 Revision 2.
Audit Logs about the handling and use of PII data, including Logs that track PII Extracts and Logs containing PII Data	At least ninety (90) days online; ten (10) years for archiving old records	OHIP retains audit records and logs online for a minimum of ninety days (90) days and archives old records for ten (10) years[46] to support after-the-fact investigations of security incidents and to comply with regulatory and organizational information retention requirements for logs containing PII data and for logs tracking the handling and use of PII data. Additionally, the organization handles and retains information within the information system and information output from the system by applicable state and federal laws, directives, policies, regulations, standards, and operational requirements. Implementation Standards: Retain output, including, but not limited to, audit records, system reports, business and financial reports, and business records, from the information system for ten (10) years or in accordance with the Administering Entity's organizational requirements, whichever is more restrictive.	To be compliant with the HIPAA, NIST SP800-66 Revision 2, and the latest version of ARC-AMPE[47] 42 CFR § 431.17 - Maintenance of records General Records Schedules (GRS) 4.2.140 OMB M-07-16 (May 22, 2007), Exhibit 1, Section C, bullet "Log and Verify"
Logs of System access records (Systems not requiring special accountability for access)	Three (3) months or until business use ceases	OHIP retains logs of system access records of systems that do not require special accountability for access (e.g. public facing Provider lookup solution, non-production environment with de-identified test data, internal project tracking tool) and retains these records for three (3) months or until the business use ceases. These records are used to monitor inappropriate systems access by the user.	

[46] ARC-AMPE Volume 2 Reference

Log or Data Type	Retention Period	Policy Statement	Regulation
Logs of System access records (Systems requiring special accountability for access)	Six (6) years after the password is altered or the user account is terminated	OHIP retains logs of system access records of systems requiring special accountability for access (e.g. systems where access to the system create privacy or financial risk, user activity **MUST** be re-constructible, or contains sensitive data, etc.). In these cases, OHIP retains these records for six (6) years after the password is altered or the user account is terminated. These records are used to monitor inappropriate systems access by the user.	
Logs of IT M&O records	Three (3) years after agreement, control measures, procedures, the Project, activity, or transaction are obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use	OHIP retains logs until three (3) years after agreement, control measures, procedures, the Project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use of IT operations and maintains records. These records relate to the activities associated with the M&O of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes the activities associated with IT equipment, IT systems, and storage media, IT system performance testing, asset and authorized staff configuration management, Change Control, and maintenance on network infrastructure.	
Logs of Technical and administrative help desk operational records	One (1) year after resolution, or when no longer needed for business use	OHIP retains logs until one (1) year after resolution, or when no longer required for business use, of operational records of technical and administrative help desks created or received while managing administrative, technical, and IT help desks.	General Retention and Disposition Schedule for NYS Government Records - 90255
Logs of Public Customer service operations records.	One (1) year after resolution, or when no longer needed for business use	OHIP retains logs until one (1) year after resolution, or when no longer required for business use of public customer service operations records, which the agency creates or receives while providing customer service to the public.	
Logs related to IT services performance records	One (1) year after the SLA, procedures, or measures is/are superseded OR terminated	OHIP retains logs of events/activities related to IT service performance records until one (1) year after the SLA, procedures, or measures is/are superseded OR terminated.	Adapted from: NARA 810 IT Services Performance

Log or Data Type	Retention Period	Policy Statement	Regulation
Logs related to Help Desk Monitoring (All records except Contractor performance-related monitoring records)	Three (3) months or no longer needed	OHIP retains logs of events/activities related to Help Desk Monitoring for all records except Contractor performance-related monitoring records for three (3) months or until no longer needed for review and analysis.	Adapted from: NARA 811-1 Help Desk Monitoring
Logs related to Help Desk Monitoring (Contractor performance-related monitoring records)	Three (3) years after the agreement, procedures, or measures is/are superseded OR terminated	OHIP retains logs of events/activities related to Help Desk Monitoring for all Contractor performance-related monitoring records until three (3) years after the agreement, procedures, or measures is/are superseded OR terminated.	Adapted from: NARA 811-2 Help Desk Monitoring
Logs related to Monitoring System Usage	Three (3) years or until business use ceases	Electronic and manual records used to document and calculate costs and to bill program units for computer usage and IT services. These records are also used for cost recovery, budgeting, or administrative purposes. Minimum Retention and Disposition: Destroy three (3) fiscal years after creation. Justification: Chargeback records are needed for three (3) fiscal years for budgetary purposes and, if used for cost recovery or billing purposes, to comply with audit requirements.	General Retention and Disposition Schedule for NYS Government Records - 90224
Logs related to the IT Security Audit of data unrelated to FTI, PII, or PHI data. Refer to Audit logs above for FTI, PII, or PHI data	Three (3) months or until business use ceases	OHIP retains logs of events/activities of the IT Security Audit of data unrelated to FTI, PII, or PHI data for three (3) months or until business use ceases.	Adapted from: NARA 817-5 IT Security GRS 3.2.030
Other Production Logs and logs with Production Data not mentioned above, and do not contain any Sensitive Data	Minimum of three (3) months	Within local systems (unless business requirements deem it necessary to keep longer) or within the consolidated log infrastructure, logs of events/activities related to production data **MUST** be maintained and readily available for at least three (3) months. Based upon requirements, including audit or legal needs, logs **MAY** need to be retained for longer. Exceptions to this include other logs in previous statements within this retention standard document: • Logs of or related to FTI, PHI, and/or PII	

Log or Data Type	Retention Period	Policy Statement	Regulation
		• Logs with Credit Card and Purchasing Card Information • Logs of System access records • Logs of IT M&O records • Logs of public customer service operations records • Logs related to IT services performance records • Logs related to Help Desk Monitoring • Logs associated with the Monitoring System Usage • Logs related to the IT Security Audit of data not associated with FTI, PII, or PHI data	
Logs in all Non-Production Environments not containing Production Data or Sensitive Data.	Minimum of three (3) months	The organization retains logs of events/activities related to non-production and non-sensitive data for at least three (3) months.	

6.0 Ongoing Licensing and Support Standard

6.1 Introduction

The Ongoing Licensing and Support Standard establishes the mandatory requirements for procuring, licensing, maintaining, and transitioning all third-party software, tools, and solutions (collectively, 'Third-Party Technology') integrated into the OHIP MES. Every MES solution depends on commercial and open-source components whose licensing terms, support agreements, and lifecycle decisions directly affect system availability, security posture, and OHIP's long-term operational continuity.

This standard governs the full software lifecycle, from initial justification and cost modeling through procurement, licensing, ongoing maintenance, audit, and eventual transition or decommissioning. It requires Contractors to ensure that all licensing rights, source code access, and transition plans are structured to protect OHIP's interests in the event of Contractor disengagement, product end-of-life (EOL), or technology obsolescence. Requirements address total cost of ownership (TCO) assessment, security and compliance oversight, training and knowledge transfer, escalation protocols, and exit planning.

Compliance with this standard is required for CMS SMC and supports OHIP's eligibility for enhanced FFP under 42 C.F.R. § 433.112 and operational FFP criteria under 42 C.F.R. § 433.116. Associated deliverables and artifacts are located in Appendix A.

6.2 Objectives

The primary objectives of this Standard are to:

- Ensure NYS secures the necessary ownership, licensing rights, and long-term access to all MES solutions.
- Govern the procurement, implementation, support, and decommissioning of third-party components including open-source software (OSS) and specialized tools.
- Outline required life-cycle activities, from justification and cost modeling through licensing, maintenance, and transition, for all new software procurements.
- Ensure all license agreements and transition plans are structured to support seamless transitions between Contractors and long-term operational continuity.
- Align with federal funding requirements, including Conditions for Enhanced Funding (CEFs) under 42 C.F.R. § 433.112 and operational FFP criteria under 42 C.F.R. § 433.116, particularly those related to licensing, system reuse, and sustainability.

All MES solutions and third-party software governed by this standard **MUST** comply with all:

- CMS SMC Outcomes and Metrics, including security (Outcome #14), risk management (Outcome #16), and continuous improvement (Outcome #17).
- Applicable NYS policies, including risk management (NYS-S14-001), security (NYS-S14-005, NYS-S15-003, NYS-P03-002), secure development life cycle (NYS-S13-001), and secure coding (NYS-S13-002).

> 📝 ***Note:*** *Contractor engagements executed through the NYS Office of General Services (OGS) IT Umbrella Contracts–Manufacturer Based (Statewide) contract are legally binding, and all Contractors* ***MUST*** *adhere to all terms and conditions.*[48]

6.3 Roles and Requirements

OHIP holds ultimate authority and responsibility for all decisions related to the selection, use, and life cycle management of MES solutions and integrated Third-Party Technology. OHIP's governance prerogatives include the following:

- Retains final approval authority for any MES solutions developed or Third-Party Technology proposed by a Contractor for use within the OHIP MES environment or for broader Medicaid operations.
- Validates any Proof of Concept, pilot results, or integration tests before granting permission to move forward with procurement or production use.[49]
- Is named as the primary licensee or assignee in all third-party software agreements.
- Retains sole and irrevocable ownership of all Medicaid-related data accessed, processed, or stored by MES solutions and third-party software/solutions/technology tools.[50]
- Monitors Contractor compliance and performance throughout the contract.
- Verifies that all required documentation (such as SLAs, warranties, risk assessments and security attestations) are submitted and maintained.
- Monitors Contractor performance against agreed-upon metrics and ensures that the Contractor actively participates in governance forums, risk mitigation efforts, and operational reviews.[51]

The Contractor's specific obligations under this governance framework are defined in Sections 6.3.1 through 6.13.

6.3.1 OHIP Contractor Role Requirements

The Contractor **MUST**:

- Align procured NYS MES components with the NYS Medicaid program's business, regulatory, and performance expectations.
- Operate in accordance with CMS regulations for enhanced funding, NYS governance policies, and OHIP MES Standards.
- Conduct appropriate market research to identify and present software options that meet OHIP's business needs and technical requirements per the applicable regulations.

---

[48] For more information, please see OGS IT Umbrella Contracts – Manufacturer Based (Statewide)
[49] For more information, refer to the OHIP Solution Delivery Domain Document, Release Management Standard and Test Management Standard.
[50] As seen in CMS's Enhanced Funding Conditions, including data ownership and reusability mandates outlined in 45 C.F.R. §95.617, which prohibits proprietary control over systems funded with federal matching dollars.
[51] This oversight is anchored in compliance with CMS certification outcomes and NYS IT governance standards: NYS-P03-002, NYS-S14-001, NYS-P13-001, and NYS-S13-001.

- Handle user-inquiries, triage incidents, perform root cause analyses or assessments, and escalate issues as needed, providing Tier 1 and Tier 2 support.
- Act as the primary liaison between OHIP and any third-party technology provider, including coordinating onboarding tasks such as user provisioning, access configuration, and initial data exchange setup.
- Initiate and manage escalations, coordinating with third-party technology providers as needed if technical issues arise.
    - Obtain, maintain, and make accessible to OHIP all documentation and agreements with a legal or operational context pertaining to Contractor-developed MES solutions or third-party sourced technology.

6.3.2 Third-party Technology Provider Role Requirements

The Contractor **MUST** ensure, through contractual terms with its Third-Party Technology providers, that such providers:

- Deliver and maintain the core software under the licensing terms facilitated through the Contractor.
- Supply updates, bug fixes, security patches,[52] and enhancements that address known vulnerabilities, emerging threats, and evolving functional requirements.
- Honor warranty coverage with clear provisions for the resolution of software defects or performance failures that compromise system functionality or availability.
- Join triage calls or live working sessions to assist in diagnosing and resolving problems when issues exceed the Contractor's Tier 1 or Tier 2 support capacity, or when remediation requires deep product expertise.
- Make SMEs available to clarify configuration complexities, address performance inconsistencies, or mitigate integration incompatibilities.
- Collaborate with the Contractor and OHIP to support timely remediation of vulnerabilities or defects.[53]

[52] Security patches should be supplied in the timeframe established in the OHIP Infrastructure and Operations Standard, Infrastructure Management Standard.
[53] These collaborations are in accordance with the NYS Establishing Technology Solutions and Standards policy (NYS-S13-001) and federal privacy and security frameworks, such as CMS's Acceptable Risk Controls for ACA, Medicaid, and Partner Entities (ARC-AMPE).

6.4 Software Approval Process

6.4.1 Initial Justification

Before any MES solution development or third-party procurement activity, the Contractor **MUST** develop and submit a comprehensive business case/justification that:

- Clearly demonstrates the business value of the proposed solution, including how it advances one or more OHIP strategic objectives, such as improved access to care, administrative efficiency, stakeholder engagement, or compliance with CMS and NYS Medicaid program mandates.
- Is tailored to the operational or functional context of the proposed software.
- Implicitly or explicitly links the proposed software to the Advance Planning Document (APD) that has been approved by CMS with specific reference to the relevant MES solution, outcome, or performance metric defined in the APD scope.
- Cites the CMS-approved funding rationale and identify how the software will contribute to the success of that scope, particularly in cases where enhanced federal funding (e.g., 90/10 or 75/25 match) is being claimed.[54]
- Documents where the proposed software supports modular design, interoperability, or data reuse in alignment with CMS SMC outcomes.
- Explains why existing MES OHIP-owned or supported systems, tools, or platforms are not viable or sufficient for the task at hand, providing evidence, such as the results of reuse evaluations, limitations of past pilot efforts, or constraints related to scalability, licensing, or system interoperability.
- Presents an initial risk mitigation overview that outlines how adoption of the proposed Third-Party Technology will address known challenges, whether those relate to system compliance gaps, regulatory risks (such as HIPAA violations), infrastructure performance limitations, or inefficiencies that drive up operational costs.
- Describes how the Third-Party Technology reduces future technical debt or enhances long-term maintainability, where applicable.

6.4.2 Documentation Requirements

To obtain approval for the Third-Party Technology, the Contractor **MUST** submit a comprehensive documentation packet that includes:

- A detailed datasheet that describes the product's core capabilities, supported technologies and environments (e.g., browsers, operating systems, and databases), integration points, deployment models (e.g., Software as a Service [SaaS], on-premises, and hybrid), and Roadmap for version updates.
- A full draft of any applicable Master Licensing Agreements (MLAs), End-User Licensing Agreements (EULAs), or subscription contracts that define the Third-Party Technology usage rights, pricing models, ownership and renewal terms, termination clauses, and data access or restriction provisions.

---

[54] Refer to the FFP Regulation 42 C.F.R. §433.112.

- Documentation that demonstrates OHIP retains all necessary rights to use, configure, customize, and transition the software without incurring proprietary constraints[55] and confirms that licenses are assignable or transferrable to OHIP.[56]
- Security and Privacy Compliance Documentation[57] that demonstrates Third-Party Technology adheres to both CMS and OHIP information security and privacy standards.
- The TCO estimate for the proposed Third-Party Technology's intended life cycle, including all anticipated costs associated with acquisition, implementation, integration, licensing, hosting (if applicable), maintenance, support services, training for OHIP personnel, and eventual termination or transition. The TCO estimate **MUST** be consistent with CMS APD policies and FFP rules.[58]

6.4.3 Proof of Concept

The Contractor **MAY** be required to submit a Proof of Concept for its solution that **MUST**, at minimum:

- Be scoped collaboratively with OHIP.
- Replicate key operational scenarios that demonstrate the Third-Party Technology's ability to support essential, targeted NYS Medicaid functions.
- Be executed in a non-production environment that closely mirrors the intended OHIP production infrastructure and includes realistic test data and technical conditions representative of the NYS MES ecosystem (e.g., integration endpoints, authentication mechanisms, and system constraints).
- Be observed and reviewed by business owners, system architects, IT security staff, and compliance personnel for performance, risks, and compliance with State and federal requirements.
- Be evaluated based on well-defined criteria that demonstrate operational fitness and compliance (e.g., integration feasibility with existing OHIP MES components and NYS data exchange layers).
- Be tested for scalability and performance using simulated or stress-test scenarios that replicate high transaction volumes, concurrent users, or large data sets.
- Validate that the Third-Party Technology will perform reliably in production-scale environments.
- Be evaluated against Section 508 and Americans with Disabilities Act (ADA) requirements and OHIP usability standards, ensuring equitable access for all users, including those with disabilities.[59]
- Comply with CMS SMC outcomes, specifically those concerning data ownership, configurability, and system auditability.
- Be formally documented, including configuration steps, test results, issues encountered, mitigations implemented, and final recommendations, as part of the final approval package.

---

[55] Refer to 45 C.F.R. §95.617.
[56] Refer to NYS ITS Policy NYS-P08-001.
[57] For more information, refer to the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard.
[58] Refer to 42 C.F.R. §433.112.
[59] For more information, refer to the OHIP Solution Delivery Domain Document, Usability and Accessibility Standard.

Documentation will be retained as a component of OHIP MES certification evidence for audit and review by CMS.

6.4.4 Formal Approval Gate

Before procuring, deploying, or funding a Third-Party Technology under CMS federal matching provisions, whether at the 90/10, 75/25, or other enhanced funding rates, the tool **MUST** pass a formal approval gate. To pass the approval gate, the Contractor **MUST**:

- Submit the materials that support the tool (licensing, security, cost), risk assessments, and, where required, results from any Proof of Concept or pilot testing) to OHIP, who will perform a structured and impartial review to confirm that the software aligns with the business objectives outlined in OHIP's APD and that the proposed acquisition adheres to CMS's enhanced funding conditions.
- Make tool approval decision outcomes and official artifacts available to OHIP for review during CMS certification engagements, audits, or APD progress reviews.
- Ensure all approvals are traceable to defined entries in the OHIP APD library and MES solutions inventory, with clear linkage between CMS-funded outcomes and the tools used to achieve them.
- Submit the solution for re-approval **SHOULD** it undergo a significant change in scope, cost, licensing terms, or Contractor relationship.

6.5 TCO Assessment

All proposed software/solutions/technology tools **MUST** be evaluated using a comprehensive TCO assessment. The assessment **MUST** align with CMS expectations for life cycle planning under the SMC Guidance.[60]

6.5.1 Required Elements of TCO Assessment

The Contractor **MUST** submit a comprehensive TCO analysis that reflects the full financial footprint of the solution across its intended life cycle, typically five to seven years and includes the following:

- A clear breakdown of license fees, distinguishing between one-time and recurring charges, including initial costs to acquire or subscribe to the Third-Party Technology, whether through perpetual or term-based licensing.
- Explanation of pricing models, whether fees are based on per-user, per-transaction, or per-core usage, and identification of any embedded pricing escalators or volume thresholds that could increase future costs.
- An itemized list of all implementation and configuration costs, including labor and material costs for installing the Third-Party Technology, developing necessary interfaces, and configuring the solution within the NYS MES environment. Special attention **MUST** be paid to activities, such as data migration, API enablement, or solution integration, which **MAY** require dedicated consulting resources or third-party integration partners.
- A detailed description of Maintenance and Support Agreements, including both the financial terms and the technical scope.

[60] Relates to Outcome #17: Ongoing Improvement and Outcome #16: Risk Management.

- Disclosure of monthly or annual support fees, the tiered levels of support available (e.g., Tier 1 and Tier 2), and a summary of services included in each tier.
- Identification of SLAs and escalation paths for incident resolution, including commitments around patching, version upgrades, bug fixes, and service outages. Where support services are fulfilled through a third-party technology provider, the Contractor **MUST** still account for the pass-through costs and responsibilities in its TCO presentation.
- Disclosure of any scheduled or required version upgrades, platform migrations, or re-certification events that **MAY** occur during the term. If license renewals involve additional fees or re-negotiation, those anticipated costs **MUST** be clearly estimated. In cases where an upgrade requires re-integration, or results in material architectural changes (e.g., discontinuation of legacy APIs), the Contractor **MUST** budget for associated labor and testing.
- An estimate of training and onboarding costs, including end-user training, training for personnel who will be responsible for system administration, configuration, and troubleshooting, instructor-led sessions, eLearning content, training materials, knowledge transfer activities, and the effort required to transition knowledge in the event of Contractor replacement.
- An EOL replacement strategy with an estimate of the costs associated with decommissioning the Third-Party Technology, including secure data extraction, archival of relevant records, removal from production environments, and disposition of licenses or hardware (if applicable).
- Strategies for mitigating Contractor lock-in, preserving OHIP's ability to maintain modularity across the MES ecosystem, and avoiding technical or contractual barriers that hinder future adaptability.

6.5.2 Life Cycle-Based TCO Calculations

The Contractor **SHOULD** calculate the TCO for all proposed software/solutions/technology tools (including third-party provided) over an OHIP-defined life cycle that aligns with the anticipated useful life of the Third-Party Technology and funding and certification considerations. Dependent on the life cycle defined, the Contractor **SHOULD** conduct:

- **5-Year TCO Horizon:** For COTS tools or SaaS platforms that are frequently updated by the Contractor, typically subject to externally driven version changes or evolving subscription models, a five-year TCO horizon is generally appropriate.
- **7-Year TCO Horizon:** For a more foundational or embedded Third-Party Technology, such as rules engines, middleware platforms, workflow engines, or provider management modules, a seven-year life cycle is typically required.

For all TCO assessments, the Contractor **MUST** account for, at a minimum:

- OHIP's CMS-approved APDs and funding coverage for the duration of the solution/technology tool's complete life cycle.
- Modular certification timelines, including the staged release and testing cycles associated with CMS's SMC process.
- Realistic technology refresh cycles with analysis of and reference to available historical implementation and renewal trends observed across the OHIP MES technology landscape.
- Transparent documentation of all cost assumptions used in the TCO calculation, including projected inflation-based rates, usage-based pricing tiers, assumptions about user or transaction

growth, license renewal schedules, and the terms under which escalations or volume discounts apply.

- Scenario-based TCO modeling to illustrate the impact of changes in scope or scale (e.g., the potential cost impact of adding more users, expanding the solution to new modules, or increasing data throughput).

6.6 Licensing and Ownership

The Contractor is responsible for establishing and securing license agreements that not only comply with operational requirements but also safeguard OHIP's ownership rights, preserve the NYS Medicaid program continuity, and uphold CMS and NYS DOH compliance expectations.

6.6.1 Software Licenses

The Contractor **MUST** ensure that all MES-related Third-Party Technology licenses and all third-party technology licenses acquired through Contractor engagements are:

- Issued in a manner that secures OHIP's legal and operational control over the licensed products.
- Executed in the legal name of the OHIP wherever commercially and contractually feasible.

OHIP **MUST** be the primary subscriber or authorized entity of subscription-based solutions such that licensing credentials (e.g., user access rights, admin control panels, and API keys, etc.) can survive the termination of the Contractor's engagement. All licensing documentation **MUST** clearly define OHIP's rights of transfer and termination.

Software license Contracts **MUST**:

- Explicitly articulate the OHIP right to assign licenses to the successor Contractor, internal teams, or alternative operational units.[61]
- Outline the conditions under which OHIP **MAY** terminate the license without penalty, such as in cases of system retirement, Contractor nonperformance, or material breach.
- Disclose any usage restrictions, including user caps, licensing limitations, or concurrent access rules, for review by the Department's legal and procurement officials.
- Guarantee that OHIP has the legal and technical right to reuse licenses, and that the Contractor will not impose artificial barriers, such as proprietary lockouts or dependency on hosted credentials, that would impede such transitions.

OHIP retains the right to transfer access credentials, software entitlements, or digital license keys when a Third-Party Technology transitions to a new integrator, managed services provider, or internal team. All license-related provisions **MUST** adhere to OHIP's requirement for clear protections for continuity of operations, license portability, and contractual flexibility. These requirements align with the CMS CEFs, particularly those related to ownership, reuse, and system sustainability.[62]

[61] Refer to NYS-P08-001.
[62] Per 45 C.F.R. §95.617 and the SMC Framework.

6.6.2 Ownership Rights

OHIP ownership rights include, but are not limited to:

- Sole and perpetual ownership of all NYS Medicaid-related data that is stored, transmitted, or processed by any Third-Party Technology.
- Member enrollment and eligibility records, claims and encounter data, provider profiles, financial transactions, audit logs, and metadata related to service delivery.
- Full ownership of all customizations and configurations developed under the Contract.
- Any application logic, scripts, workflows, parameterizations, or middleware developed during implementation, even if built on a commercial software platform.

The Contractor **MUST**:

- Formally codify OHIP ownership of all operational assets and intellectual property generated or utilized during system development, implementation and use in all contracts, licenses, and service agreements to ensure CMS compliance,[63] minimize Contractor lock-in risk, and support OHIP's duty as steward of NYS Medicaid data.
- Acknowledge OHIP's exclusive ownership rights.
- Guarantee unrestricted access to raw and processed data, including access through export utilities, APIs, or secure database connections.
- Be contractually prohibited from using OHIP's data for any secondary, commercial, or analytical purposes without explicit written authorization.
- Comply with federal privacy and security regulations, including HIPAA, 42 C.F.R. Part 2 (which governs substance use disorder data confidentiality), relevant CMS SMC Security Outcomes, particularly those related to data sovereignty, breach response, and audit readiness, and NYS Policies and Standards to include ITS-P19-002 "Cloud Computing Policy."[64]
- Provide comprehensive documentation of all configurations, including configuration files, decision tables, access control policies, and system behavior logic.
- Deliver access to source code, object definitions, or parameter settings necessary to support future re-deployment or reuse, where applicable.[65]

6.7 Support and Maintenance Governance

The Contractor **MUST**:

- Maintain clearly defined, measurable, and enforceable support and maintenance protocols, collaborating with third-party technology providers when solutions include third-party technology to promote proactive issue resolution, minimize system downtime, and uphold the performance standards required for continued FFP.[66]

---

[63] Per 42 C.F.R. §495.360(a).
[64] For more information, refer to ITS Cloud Computing Policy.
[65] This obligation supports the CMS Federal Reuse Requirement under 45 C.F.R. §95.617, which mandates that federally funded systems be designed and documented in a manner that promotes transferability and reuse.
[66] Per 42 C.F.R. §433.116 and CMS SMC Outcomes.

- Establish a formal SLA with OHIP that covers Contractor-developed MES solutions as well as any third-party technology managed by the Contractor on OHIP's behalf.
    - Each SLA **MUST** clearly define expectations around system availability, uptime guarantees, and support responsiveness, including tiered response and resolution timeframes based on incident severity levels. The SLA **MUST** outline OCM protocols for routine Third-Party Technology updates, emergency patches, and scheduled maintenance windows, and **MUST** identify clear communication pathways for notifying stakeholders of outages, delays, or system recovery activities.
    - SLA provisions **MUST** align with CMS SMC Outcome #17, which requires that MES solutions demonstrate continuous operational improvement through metrics, performance tracking, and transparent documentation. In addition, SLA commitments **MUST** comply with NYS ITS Policies,[67] which establish standards for recoverability, continuity of service, and incident responsiveness in Department-supported IT systems.

> 📋 ***Cross-Reference:*** *The structure and content of SLAs, including availability, uptime, and tiered response and resolution commitments, are governed by Service Level Management (Section 2.5.16); specific SLA commitments are established through procurement at contract award. This section addresses Third-Party Technology-specific SLA considerations and does not redefine the SLA framework.*

- Define and maintain a detailed incident escalation pathway, documented in a formal matrix and shared with OHIP.
    - The escalation matrix **MUST** delineate tiered support roles, with the Contractor responsible for Tier 1 support (e.g., help desk, issue triage, and first-level troubleshooting) and the third-party technology provider responsible for Tier 2 support (e.g., product-level bug fixes, patches, and code-level diagnostics).
    - The escalation pathway **MUST** outline incident handoff procedures, define response triggers that elevate issues to OHIP leadership, and include designated points of contact for urgent or high-impact events, such as system outages, data integrity failures, or security breaches.
- Implement a consistent process for periodic reporting to OHIP on Third-Party Technology maintenance and performance outcomes.
- Submit maintenance and service reports on an OHIP-defined cadence.
    - Submitted reports **MUST** include an evaluation of SLA compliance, including agreed-upon issue resolution timeliness and uptime thresholds. Reports **MUST** also include ticket volume, incident severity distribution, average time to resolve issues, and descriptions of scheduled maintenance events, along with their results.
- Document any recurrent issues or systemic service disruptions along with proposed remediation plans.

> 📋 ***Cross-Reference:*** *Incident management processes and SLA governance are established in Sections 2.5.5 and 2.5.16.*

[67] Refer to NYS-P03-002, NYS-S14-001, and NYS-P13-001.

6.7.1 Maintenance Scheduling Coordination and SLA Performance Monitoring

The Contractor **MUST**:

- Understand that all MES solutions and third-party technology maintenance activities, including version upgrades, patch deployments, and infrastructure adjustments, are subject to formal OHIP review and approval before implementation.
- Submit detailed maintenance plans and schedules to OHIP for evaluation.
- Comply with the OHIP Program and Project Management Domain Document, Technical Change Control Standard.
- Document Rollback Plans to ensure recoverability in the event of failure or regression.[68]
- Strategically schedule maintenance activities to avoid conflicts with critical NYS Medicaid business cycles, as disruptions could jeopardize critical business operations or compromise federal reporting obligations.
- Engage in recurring performance meetings with designated OHIP stakeholders to review SLA metrics, discuss any deviations, and identify opportunities for improvement.
- Formalize reviews through meeting records, performance dashboards, or documented action plans.[69]

6.8 Security and Compliance Oversight

The Contractor **MUST**:

- Comply with the security and privacy policies and controls and all other applicable NYS and federal laws, regulations, policies, and standards for IT systems that transfer, process, or store OHIP data.
- Demonstrate compliance with OHIP security and privacy requirements by providing documentation and artifacts that demonstrate that applicable standards and controls are implemented correctly, operating as intended, and producing the desired outcome.[70]

> 📝 ***Cross-Reference:*** *The authoritative source for security and privacy requirements is the OHIP Security, Privacy, and Compliance Domain Document.*

[68] These practices are essential to maintaining operational control and auditability, as required by CMS SMC Outcomes #14 (Security) and #17 (Ongoing Improvement) and are consistent with NYS ITS policy directives, such as NYS-S13-001.
[69] Continuous oversight aligns directly with CMS SMC Outcome #17.
[70] Refer to the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard for more information.

6.9 Integration and Interoperability[71] Requirements

All Third-Party Technology used in the NYS MES environment **MUST** be capable of standards-based integration with existing MES solutions and enterprise platforms, including E&E, claims processing, provider and member management, and care coordination systems.

The Contractor **MUST** comply with CMS, ONC, and OHIP interoperability requirements when exchanging clinical, eligibility, or claims data with health care entities or federal systems.[72]

> 📋 ***Cross-Reference:*** *Detailed integration standards, including API governance, national data exchange standards (HL7, FHIR, X12 EDI), EDA, and protocol requirements are governed by Section 3.0.*

6.10 Training and Knowledge Transfer

Training and Knowledge Transfer supports both ongoing M&O and the Transition-In and Transition-Out activities described in Section 6.13. The requirements in this section apply across those contexts, not solely to third-party technology.

All Contractor-developed MES solutions and technology procurements and implementations **MUST** include a comprehensive training and knowledge transfer strategy as part of the contracted scope of work.

> 📋 ***Cross-Reference:*** *Enterprise knowledge management requirements are governed by Section 2.4.5.*

6.10.1 Components of Training

The Contractor **MUST**:

- Deliver tailored training sessions that enable end-users to perform routine functions, interpret system messages or logs, and resolve common issues without needing Contractor intervention.
- Provide instruction on how to utilize available diagnostics or support dashboards using role-specific content with tailored curricula for program managers, IT administrators, technical support teams, and compliance or governance personnel involved in oversight.[73]
- Deliver a full suite of up-to-date and well-organized documentation to support NYS Medicaid operations and future Contractor transitions. This includes user manuals, quick-reference guides, and system-specific SOPs that align with the OHIP's established workflows and business processes.

---

[71] Interoperability is a foundational requirement of CMS modularity principles and a key funding and certification criterion under CMS's SMC Guidance and 42 C.F.R. §433.112(b)(13). For more information on interoperability, refer to the OHIP Solution Delivery Domain Document, Data and Information Domain Document, and the Security, Privacy, and Compliance Domain Document.
[72] Refer to the OHIP Data and Information Management Domain Document, Data Conversion Standard.
[73] This user-focused training approach is supported by CMS's expectations for ongoing operational control, as outlined in CMS SMC Outcome #17 (Ongoing Improvement) and Outcome #15 (State Operational Readiness).

- Provide complete configuration documentation detailing environment variables, customizable parameters, deployment instructions, and relevant architectural dependencies for technical users.

All training materials and documentation **MUST** be provided in editable, version-controlled digital formats to ensure traceability and enable future updates. These materials are considered deliverables under the Contract and **MUST** be clearly licensed or assigned to OHIP, consistent with federal reuse guidance under 45 C.F.R. §95.617.

The Contractor **SHOULD**:

- Provide comprehensive training and structured knowledge transfer for designated OHIP staff with the operational proficiency to use the Third-Party Technology independently.

6.10.2 Training Schedule

The Contractor **MUST**:

- Complete initial training prior to the solution go-live date.
- Formally validate initial training for the solution through the State's Operational Readiness Review (ORR) process.
- Ensure that all relevant training sessions are delivered on schedule and that a completion checklist, verifying attendance and proficiency, is reviewed and signed off by designated OHIP personnel.
- Vet and obtain OHIP approval for all training curriculums, materials, schedules, and recommended attendee lists, whether original compilations or subsequent updates, prior to roll out within the Agency.
- Provide refresher or delta training following any major version upgrade, UI change, or material configuration adjustment.
- Support long-term knowledge retention by offering periodic workshops, access to searchable knowledge bases, or helpdesk-integrated training modules.

6.11 Contractual Controls and Escalation

OHIP retains ultimate authority and oversight over all Contractor-developed MES solutions and third-party technology used to support NYS-funded operations. This includes clearly defined contractual rights and escalation mechanisms to mitigate operational disruptions, ensure performance standards are upheld, and provide a direct path for OHIP intervention when Contractor management proves insufficient.

The controls in this section uphold compliance with 42 C.F.R. §433.112 and §433.116, which require NYS to retain ownership, control, and accountability over NYS Medicaid solutions receiving enhanced federal funding. In addition, the provisions conform with NYS ITS procurement, contract, and risk management standards including Information Security Risk Management (NYS-S14-001) standards.

6.11.1 OHIP Oversight Controls

OHIP retains explicit authority to:

- Preserve the integrity, sustainability, and compliance of the NYS MES ecosystem by terminating or discontinuing use of a Contractor-developed MES solution or integrated third-party technology,

exercising an NYS OHIP-directed contract exit clause, and/or engaging in direct intervention with a third-party technology provider.

- Terminate the use of any Contractor-developed MES solution or third-party technology that fails to comply with established performance, security, or cost-effectiveness thresholds to align with NYS Medicaid obligations for ongoing improvement (Outcome #17) and security (Outcome #14).
- Terminate the use of any Third-Party Technology that underperforms against established SLAs, violates privacy or cybersecurity policies, such as HIPAA, CMS ARC-AMPE, or NYS-ITS-802.11 Wireless Network Security (NYS-S15-003), or demonstrates unanticipated and unjustifiable cost escalations that exceed approved TCO thresholds.
- Invoke termination as part of a broader CAP if the Contractor fails to correct known deficiencies despite receiving formal notification and reasonable remediation time, or if CMS certification or FFP is jeopardized.
- Directly engage a third-party technology provider in instances where Contractor coordination, communication, or support management is deficient.
- Bypass OHIP Contractor-led channels to access performance metrics, incident logs, patch schedules, or technical support from the third-party technology provider.
- Convene parties for joint triage or escalation meetings to address service degradation or critical defects.

All Contracts **MUST**:

- Include tri-party or Contractor-mediated agreements that preserve OHIP's access to third-party support lines, configuration data, and governance communications.
- Empower OHIP to execute termination actions without financial penalty where clauses permit and **MAY** enact a managed disengagement strategy to ensure continuity of Medicaid operations and secure transfer or archiving of any impacted data.
- Structure disengagement to preserve data integrity, maintain interoperability with upstream and downstream MES modules, and mitigate risk to member or provider services.

The Contractor **MUST** cooperate fully with OHIP-directed interventions, including providing all requested documentation, access credentials, and technical support within the timeframes specified by OHIP.

6.11.2 Escalation Protocols

The Contractor **MUST**:

- Develop and submit an internal escalation protocol that outlines tiered response levels tied to incident severity, designated points of contact, and clear timelines for response and escalation.
- Identify both primary and backup personnel responsible for each escalation tier and routinely review selected personnel during OHIP-conducted performance audits or ORRs.
- Ensure the escalation protocol enables prompt escalation of critical issues to appropriate technical, managerial, and executive stakeholders within the Contractor organization to prevent service degradation and mitigate downstream risks to the OHIP MES functionality.
- Explicitly define OHIP intervention points in the escalation process, such as unresolved SLA violations, unapproved or premature Third-Party Technology deployments, repeat security incidents with ambiguous root causes, or breaches of data residency or access controls.

- At these inflection points, OHIP **MAY** require submission of CAPs, temporarily suspend use of the affected Third-Party Technology or initiate direct engagement with the third-party technology provider.
- In the event of persisting service disruptions or critical thresholds exceptions, OHIP retains the right to intervene directly.

6.12 Audit and Reporting Requirements

OHIP requires proactive Contractor reporting on operations and maintains the right to conduct audits of financial,[74] contractual, and technical[75] practices related to MES environment software/solutions/technology tools (including third-party technology). These measures are critical for ensuring the effective stewardship of public funds and adherence to the NYS Medicaid program integrity principles.[76]

The Contractor **SHOULD**:

- Document, maintain, and integrate clearly defined multi-tiered escalation protocols within a service management plan.

6.12.1 Required Reports

To support ongoing compliance, performance oversight, and funding accountability, the Contractor **MUST**:

- Provide OHIP with a robust suite of operational and financial reports.
- Map each incident against established SLA tiers, with clear documentation of response and resolution times, root cause analysis for repeated or critical failures, and a summary of emerging trends along with recommended mitigation strategies.
    - These logs will be integrated into OHIP's operational dashboards and used for contract compliance monitoring, OHIP Medicaid IT governance activities, and to satisfy CMS reporting obligations such as MACPro milestone updates and certification evidence submissions.
- Deliver a comprehensive license and support utilization report on a cadence agreed upon with OHIP.
- Detail the distribution and activation status of Third-Party Technology licenses across all user categories, identify any over-licensing or under-utilization patterns, and highlight anomalies in access controls.
- Summarize support interactions managed by the third-party technology provider, including the volume and types of support requests, resolution times, and service trends.

---

[74] Refer to Section 7.0.
[75] Refer to the OHIP Solution Delivery Domain Document, the OHIP Data and Information Management Domain Document, and the OHIP Security, Privacy, and Compliance Domain Document.
[76] These requirements support the CMS SMC framework, particularly Outcome #17 (Ongoing Improvement) and Outcome #16 (Risk Management), and are necessary to sustain FFP under 42 C.F.R. §§ 433.112 and 433.116. The expectations below also conform with NYS ITS audit and procurement transparency requirements under NYS-P08-001.

- Maintain ongoing logs and make available evidence of patch management practices, and SLA compliance in alignment with the OHIP Security, Privacy, and Compliance Domain Document, Security and Privacy Compliance Standard.
- Comply with FinOps reporting requirements outlined in Section 7.0.

The Contractor **SHOULD**:

- Submit performance and issue logs on a cadence specified by OHIP that capture key service metrics, including system uptime, downtime incidents, and the volume, severity, and nature of reported issues.

6.12.2 OHIP Audits

OHIP retains the explicit right to:

- Audit all Contractor MES solution development and operationalization (including third-party technology) expenditures and associated Contractor practices to ensure fiscal accountability,[77] licensing integrity, and operational transparency.
- Examine invoices for Third-Party Technology tool costs, such as license acquisition or renewal fees, Third-Party Technology support and maintenance contracts, and any pass-through charges associated with external Third-Party Technology services.
- Conduct licensing compliance audits to verify that the number and type of active Third-Party Technology licenses align precisely with contractual entitlements and that no unauthorized, expired, or unlicensed Third-Party Technology is in use within the NYS MES environment.
- Conduct audits to confirm that license reallocations or transfers adhere strictly to NYS ITS procurement policies and OHIP MES governance frameworks.
- Review all Contractor and Subcontractor agreements that support technology implementations or operations.
- Examine contractual clauses related to data protection, security standards, service-level expectations, and responsiveness to incidents or escalations.
- Request evidence that subcontractors or third-party technology providers are meeting their defined deliverables and adhering to applicable laws and standards.

The Contractor **MUST**:

- Maintain detailed and itemized invoice records a minimum of six (6) years in accordance with the records retention requirements by the Office of the NYS Comptroller (OSC) fiscal retention policies[78] and the requirements under the federal Office of Management and Budget's Uniform Guidance (2 C.F.R. Part 200), particularly where enhanced federal funding is involved.
- Fully cooperate with both internal OHIP auditors and any external audit entities authorized by OHIP or CMS.

---

[77] For more information, refer to Section 7.0.
[78] For more information, refer to XII.3 Records Retention – Accounts Payable Vouchers and Land Claims.

6.13 Exit and Transition Planning

OHIP retains the right to ensure that all software/solutions/technology tools (including third-party technology) developed, acquired, or managed via Contractor sub-contracts include a clearly defined exit and transition plan. Exit and transition planning is a federal and NYS compliance requirement under CMS SMC Outcome #16 (Risk Management) and Outcome #17 (Ongoing Improvement).

The master Transition-Out Plan and the overall transition framework, including transition timing, knowledge transfer, and staffing continuity, are governed by the OHIP Program and Project Management Domain Document, Section 2.18 (Transition Management), which is the authoritative source for the transition framework. This section and its associated deliverables provide the operational and M&O execution of that master plan, including service continuity, data transfer, readiness reviews, status reporting, and operational knowledge transfer. Contractual and legal exit terms, such as termination and renewal provisions, are addressed through the Contract and OHIP Legal; this section governs the Contractor's operational and M&O transition-out execution.

> 📝 ***Cross-Reference:*** *Operational transition-out requirements including service continuity and data transfer are governed by Section 2.6.1.*

6.13.1 Contractor Transition Responsibilities

The Contractor **MUST**:

- Outline detailed procedures for orderly disengagement from the Contractor and/or the third-party technology provider, including termination of support contracts, decommissioning of any integrations or proprietary extensions, and identification of associated transition risks such as data loss, system dependencies, or gaps in operational knowledge within its exit and transition strategy.
- Submit the exit and transition strategy at the time of initial Third-Party Technology implementation and continue to update it throughout the term of the awarded contract to reflect any changes in licensing, platform architecture, or Contractor responsibilities.

In the event of contract termination or expiration, the Contractor **MUST**:

- Transfer all configuration artifacts, documentation, and licenses to OHIP. This includes the full body of technical and user documentation, integration schemas, parameter settings, environment configurations, customizations, and SOPs.
- Reassign all Third-Party Technology licenses to OHIP or structure them in a way that allows continued use under new Contractor arrangements.
- Ensure that the Third-Party Technology solution includes the ability to extract and export all data processed or stored by the system in accessible, unencrypted, and non-proprietary formats such as CSV, JSON, or XML.
- Accompany exports with thorough data dictionaries, schema mappings, and relevant metadata to enable efficient reloading into successor solutions.
- Facilitate exports that comply with HIPAA and NYS data security protocols, including the use of secure transfer mechanisms and validation of data integrity and completeness.

The Contractor **SHOULD**:

- Develop and maintain a comprehensive exit and transition strategy for all Contractor-developed MES solutions (including Contractor-managed third-party technology) used in the NYS MES environment.

6.13.2 OHIP Transition Planning

The Contractor **MUST** support OHIP's transition risk mitigation strategy for every Contractor-managed MES solution and Third-Party Technology operating within the NYS MES environment. The Contractor **MUST** provide OHIP with all information necessary to maintain this strategy, including documented triggers for early termination or emergency transition (such as Contractor insolvency, unresolvable technology obsolescence, repeated SLA violations, or security and compliance violations).

7.0 Cloud FinOps Standard

7.1 Introduction

The Cloud FinOps Standard establishes the mandatory requirements for achieving financial transparency, accountability, and optimization for all cloud expenditures supporting the OHIP MES. As OHIP's MES portfolio operates increasingly on cloud infrastructure, the ability to attribute costs accurately to specific contracts, business units, and federally funded projects is essential for CMS reporting, FFP cost allocation, and responsible stewardship of public funds.

This standard requires Contractors to implement cost consolidation, allocation, and tagging practices that provide granular visibility into cloud spending. It defines requirements for cost reporting, budgeting, forecasting, and optimization, including architectural isolation to prevent cost commingling across OHIP contracts. The Contractor **MUST** collaborate with OHIP's FinOps function to establish clear practices, participate in cost reviews, and support optimization efforts.

Compliance with this standard is required for CMS SMC and for OHIP's sustained eligibility for enhanced FFP. Associated deliverables and artifacts are located in Appendix A.

7.2 Objectives

The objectives of this Standard[79] are to:

- Adhere to financial requirements of the CMS and other oversight agencies.
- Achieve complete financial transparency and accountability for all cloud expenditures through consolidated reporting and cost allocation.
- Enable accurate cost attribution for all cloud services to specific contracts, business units, and federally funded projects.
- Implement architectural and tagging strategies that provide granular visibility into cloud spending patterns.

7.3 Cloud FinOps Oversight

The Contractor **MUST**:

- Develop solutions that provide for Cloud FinOps usage, traceability, and reporting requirements.
- Collaborate with State-identified resources bearing accountability for and providing oversight and direction of OHIP FinOps to establish clear practices for each OHIP solution or portfolio of solutions.
- Comply with OHIP's FinOps processes by providing the necessary cost/usage visibility, participating in relevant reviews, and supporting OHIP-led optimization efforts related to the Contractor's services.

---

[79] The FinOps Foundation defines FinOps as "an operational framework and cultural practice which maximizes the business value of cloud and technology, enables timely data-driven decision making, and creates financial accountability through collaboration between engineering, finance, and business teams."

📋 ***Cross-Reference:*** *Infrastructure-level cost management requirements for SaaS and P/IaaS are governed by Sections 4.5.2.1 and 4.5.2.2. This section establishes the enterprise Cloud FinOps framework that applies across all service models.*

7.4 Financial Transparency and Cost Management

7.4.1 Cost Consolidation

The Contractor **MUST**:

- Collect and maintain granular cost data consisting of:
    - Granular cost data provided by the service provider and all accompanying tags.
    - Usage data (e.g. number of users, number of transactions, and number of licensed seats).
- Update cost and usage data each time the service provider executes a cost update.
- Securely transmit each solution's ongoing cost data and invoices to OHIP's primary cost reporting solution for enterprise visibility.

The Contractor is encouraged, but not required, to utilize a framework, such as Focus™[80], for normalizing cost data.

7.4.2 Cost Allocation

The Contractor **MUST**:

- Provide cost data at the contract and business unit level, such that reports on each OHIP-specified environment can be used for show-back/charge-back.
- Produce cost information that facilitates:
    - Visibility into who is spending what based on reliable data sources, fostering accountability and supporting business conversations about usage adjustments. The standard aligns with the FinOps principle, "Everyone takes ownership for their cloud usage," which is enabled by allocation.[81]
    - Compliance with the OHIP requirement for clear charge-back reporting to internal budget owners and procurements. The Contractor **MUST** provide cost data in a format that enables financial staff to understand, reconcile, and pay invoices from suppliers.[82]
    - FFP allocation by separating charges associated with an approved APD and those costs that are not part of an approved APD in full compliance with Title 42 section 433.112.[83]

[80] FinOps Open Cost and Usage Specification (Focus™)
[81] FinOps Allocation Strategies (Focus™)
[82] FinOps Invoicing & Chargeback (Focus™)
[83] Code of Federal Regulations Title 42, CFR 433.112

7.4.3 Cost Visibility and Reporting

The Contractor **MUST**:

- Leverage data from account structures and usage metrics, supplemented by tag-based grouping where appropriate.
- Detail spend-trends, budget variance, and key cost drivers.
- Provide contract context, linking costs to the related contract.

- Work with OHIP to add the attribution and costs to regular OHIP cost reports or add new cost reports as required.

The Contractor **SHOULD**:

- Provide a Monthly Cloud Usage and Spend Report as dashboard content consisting of understandable cost reports, accessible by relevant stakeholders (Business, Finance, and Technical teams), where the reports:

7.4.4 Attribution and Usage Monitoring

The Contractor **MUST**:

- Comply with the monitoring requirement established by the OSC as part of Procurement and Contract Management.[84]
- Monitor and log resource usage attributable to contracts, program areas, specific staff, services, or functions as required by OHIP on a regular basis. This includes leveraging provider logs and application-level instrumentation.
- Ensure alerts are triggered when forecast costs exceed agreed limits and that evaluation of costs against forecast for the purpose of alerting **SHOULD** be at least daily.

The Contractor **SHOULD**:

- Monitor resource usage no less frequently than monthly, with sufficient frequency to detect, alert on, and manage unexpected cost and usage irregularities in a timely manner.

7.4.5 Initial Cost Estimations

For new solutions, the Contractor **MUST**:

- Base cost estimates **MUST** be calculated using all expected cloud workloads and deployment timeframes.

The Contractor **SHOULD**:

- Provide OHIP with an estimation of forecasted cloud costs, utilizing cloud estimation tools where available and provide the tool's output along with the estimations.

[84] New York State Comptroller – Contract Monitoring

7.4.6 Budgeting and Financial Tracking

The Contractor **MUST**:

- Submit a Cloud FinOps Plan that aligns spending with business priorities and identifies cost-saving opportunities.
- Define resource usage budgets for all OHIP solutions, including those with significant or variable cloud spend.
- Actively track actual usage spend against usage budgets with established processes for variance assessment, alerting, and review.

7.4.7 Cost Forecasting and Predictability

7.5 Cloud FinOps Operational Standard

The Contractor **SHOULD**:

- Establish a process for Cloud FinOps collaboration with OHIP to forecast future costs for OHIP solutions based on historical data, planned architectural changes, anticipated usage patterns (e.g., seasonal demand, new program launches), and known cost model changes.

7.5.1 Cost Optimization and Efficiency

The Contractor **MUST**:

- Conduct solution cost optimization reviews on a cadence agreed upon with OHIP. Reviews **MUST** consider cost-saving opportunities including but not limited to:
    - Right-sizing resources.
    - Evaluating and utilizing optimal pricing models (e.g., Reserved Instances, Savings Plans, and Spot Instances).
    - Identifying and eliminating waste (e.g., unused resources and idle environments).
    - Considering architectural efficiency.
- Support OHIP's ability to evaluate and utilize early pay discounts, such as reserved instances, in accordance with OSC guidance.[85]

7.5.2 Architectural Isolation

The Contractor **MUST**:

- Architecturally isolate OHIP environments (i.e., Production [PROD]/DEV/SIT, and UAT, or distinct functional components [e.g., Common Database, Developer Tools, and Common Network]) by using separate cloud accounts (e.g., Amazon Web Services [AWS] Accounts, Azure Subscriptions, or Google Cloud Platform [GCP] Projects) whenever feasible, resulting in automatically separated costs by environment clearly identified in cloud provider billing.

---

[85] New York State Comptroller – Early Pay Discounts for Procurement Contract Purchases.

> 📝 ***Cross-Reference:*** *Environment requirements (DEV, SIT, UAT, PROD, DR) are defined in Section 4.6.1.*

7.5.3 Resource Tagging

Where architectural isolation is not practical (e.g., shared services or resources within a single account), and where costs cannot be captured on an attributable “Who did what?” basis from logs, the Contractor **MUST**:

- Apply and adhere to a minimal, defined, and *policy-enforced* tagging strategy (such as using AWS Tag Policies or Azure Policy) to all cloud resources.
- Ensure that mandatory tags focus on essential identifiers that are not easily derived otherwise (e.g., Application ID or primary Cost Center).

8.0 Preferred Operational Tools Standard

8.1 Introduction

The Preferred Operational Tools Standard establishes the mandatory requirements for technology tool selection and usage across all OHIP MES Contractors. Standardizing the operational toolset reduces integration complexity, eliminates duplicate licensing costs, and ensures that all MES solutions can interoperate with OHIP's enterprise monitoring, reporting, and governance infrastructure.

This standard requires Contractors to use the tools identified in the OHIP Preferred Operational Tools List for all customized enterprise solution implementations. Where a Contractor proposes an alternate or additional tool, OHIP approval is required with documented justification. The standard also governs the use of OSS, requiring compliance with applicable NYS and industry standards for open-source security and licensing.

The current Preferred Operational Tools List is maintained in Appendix A and reflects OHIP's cloud-first strategy. Compliance with this standard is required for CMS SMC and for OHIP's sustained eligibility for enhanced FFP.

8.2 Objectives

The primary objectives of this Standard are to:

- Ensure that new technology solutions are compatible and interoperable with OHIP's existing technology stack.
- Reduce costs and avoid duplication by leveraging a standardized set of approved operational tools.
- Ensure that all technologies implemented are industry-proven, enterprise-grade, and have a well-established support model.
- Guarantee that all solutions comply with OHIP's technical and security requirements.

8.3 Contractor Tool Use

All solutions that do not fit within the definition of OHIP's SaaS model **MUST** comply with this standard. SaaS solutions are governed by the technologies listed in individual Contracts. Only the current solution version approved by OHIP is considered the preferred operational tool.

The Contractor **MUST** refer to and comply with the technologies listed in the OHIP Preferred Operational Tools List for any customized enterprise solution implementation or enhancement. OHIP publishes guidance for tool processes and use. The Contractor **MUST**:

- Ensure their team members are familiar with the published guidance and integrate the usage protocols in their workflow.
- Remain aligned with OHIP's updates or modifications to the guidance and adapt their processes accordingly.
- Obtain OHIP approval for any variation to this standard in the Contract.
- Propose and seek OHIP approval for any additional or alternate technologies other than those listed in OHIP's Preferred Operational Tools List.

A copy of this standard will be shared as an Exhibit during the procurement process. The current Preferred Operational Tools List can be found below:

Table 9 – Preferred Operational Tools List

Category	Tool	Tool Description
Data Modelling	Erwin Data Modeler	Facilitates the design, visualization, and management of data architectures. It ensures data integrity, consistency, and standardization across platforms. The tool supports collaboration among teams to concurrently develop models. It supports compliance with data governance standards and in performing impact analysis
Document Management	Microsoft SharePoint	Centralizes document storage, collaboration, and management. It is crucial for maintaining a single source of truth for documentation and fostering effective team collaboration within the modernization project. SharePoint's version control and workflow capabilities enhance document accuracy and accessibility.
IT Service Management (ITSM)	Jira Service Management	As an ITSM platform that brings together development, IT operations and business teams to coordinate and manage requests, incidents, problems, and technical changes in an integrated system.
Requirements Management	Jira	Manages project tasks, timelines, and requirements and is essential for tracking progress and ensuring projects meet set goals. Jira's flexible issue tracking system supports project transparency and accountability.
Project Management	Microsoft Project	Used to create schedules, project plans, manage resources and keep track of time. It has features such as Gantt charts, kanban boards and project calendars supporting comprehensive project management.
Security and Compliance	AWS Key Management Service	Manages cryptographic keys securely for AWS services and applications, ensuring data protection and compliance. It facilitates regulatory compliance by automating key rotation and auditing processes.
Security and Compliance	Fortify	Provides static and dynamic application security testing to identify and remediate vulnerabilities. By integrating into the development cycle, Fortify helps maintain a proactive security posture.
Security and Compliance	Tenable	Delivers continuous network monitoring to detect and respond to security threats, ensuring robust compliance with regulatory standards. Its comprehensive vulnerability assessments help prioritize and remediate risks effectively.
Source Control and Version Management	GitLab Cloud	Facilitates code versioning, collaboration, and continuous integration/continuous deployment (CI/CD) workflows. Ensures code integrity and supports

Category	Tool	Tool Description
		collaborative development within the modernization team.
Web Content Management (Web Servers)	NGINX	Delivers high-performance web server capabilities, including load balancing and media streaming. Essential for ensuring the scalability and reliability of web services within the MES. NGINX's architectural flexibility optimizes resource usage and enhances web application security.

The OHIP Preferred Operational Tools List reflects a cloud-first strategy. For on-premises solutions, the Contractor **MUST** seek OHIP's review and approval of technology usage on a case-by-case basis.

> 📋 ***Cross-Reference:*** *Infrastructure-level technology standards and cloud service requirements are governed by Section 4.7.*

The Contractor **SHOULD**:

- Follow the Open-Source Project Security Baseline and ISO/IEC 5230 if they use OSS in their solutions.

8.3.1 Open-Source Software

All OSS **MUST** be implemented in accordance with ITS-P019-005.[86]

Only the DOH Chief Technology Officer or an assigned designee **MAY** approve the use of OSS. To be reviewed, OSS **MUST** meet these four (4) minimum conditions:

- The software **MUST** be free to use.
- The source code of the software **MUST** be available on the Internet.
- The license to use the software **MUST** be approved by the DOH Division of Legal Affairs (DLA). A list of approved licenses is listed in ITS-P19-005 Appendix A: Pre-Screened Open-Source Licenses.[87]
- The user is not required to agree to terms or conditions prior to the download, or DLA has approved the terms and conditions associated with the OSS.

OSS options **SHOULD** be considered first for all potential software solutions.

The Contractor using OSS **MUST** comply with:

- ISO/IEC 5230 (OpenChain) Standard,[88] which outlines requirements for organizations to effectively manage open-source license obligations.
- OpenSSF's Application Security Verification Standard (ASVS),[89] which provides benchmarks for securing OSS.

---

[86] Refer to ITS-P19-005 more information.
[87] Refer to ITS-P19-005 Appendix A for more information.
[88] ISO/IEC 5230:2020 - Information technology—Open Chain Specification
[89] OWASP Application Security Verification Standard (ASVS) | OWASP Foundation

- Interoperability standards for data exchange and communication, such as those defined by the World Wide Web Consortium (W3C) and Cloud Native Computing Foundation, as appropriate.
- Open-source license requirements when implementing DOH-approved software.

The Contractor **MUST** also:

- Implement tools and processes to ensure adherence to open-source license types, including strong copyleft (e.g., GPL), weak copyleft (e.g., LGPL), and permissive (e.g., MIT).
- Develop and maintain comprehensive documentation that outlines how OSS is used in the solution.

> 📋 ***Cross-Reference:*** *Open-source components used in integrations must also comply with the security scanning requirements in Section 3.5 and the licensing governance in Section 6.6.*

8.4 Maintaining the OHIP Preferred Operational Tools Standard

OHIP will update the Preferred Operational Tools List periodically, including when new technology is approved or existing technology is restricted or discontinued. The Contractor **MUST** monitor for updates and align its technology usage accordingly. Changes to the Preferred Operational Tools List do not require a formal amendment to this standard; the Contractor **MUST** comply with the current version of the list as published by OHIP.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Division of Operations and Systems (DOS) and Chief Technology Office (CTO)
11 Corporate Woods Boulevard
Albany, NY 12211
Telephone: TBD
Email: TBD
Statewide technology policies, standards, and guidelines may be found at the following website:
https://its.ny.gov/policies

10.0 Revision History

The following table records the revision history of this Consolidated Domain Document. The seven component standards each maintained their own revision histories prior to consolidation. This table captures the lifecycle of the domain document from initial publication onward.

Date	Version	Author	Description of Change
06/25/26	1.0	NYS TAS	Initial publication of the OHIP Infrastructure and Operations Domain Document. Consolidates: ITSM Standard, Application Integration Standard, Infrastructure Management Standard, Log Management Standard, Ongoing Licensing and Support Standard, Cloud FinOps Standard, and the Preferred Operational Tools Standard. and incorporates compliance tiers (**MUST**/**SHOULD**/**MAY**) for all requirements.
08/17/26	1.1	NYS TAS	Added batch file exchange acknowledgement requirement (ARCH-0050, **SHOULD**): receiving systems return an

			acknowledgement for batch file exchanges, with an SDR-based exception for one-way, non-transactional distributions (Section 3.4 integration patterns; Appendix B). Corrected the Appendix B Section 3.0 tier summary to match the register (**MUST** 44 / **SHOULD** 6). Section 1.7.2 counts updated.
10/23/26	1.2	NYS TAS	Domain Document approved by DOH.

Appendices

Appendix A: Deliverables and Artifacts

The following tables identify the Deliverables and Artifacts associated with this Domain Document. Deliverables are contractually binding work products that the Contractor **MUST** submit to OHIP for formal review and approval. Artifacts are supporting work products (e.g. documentation, models, charts) that the Contractor **MUST** create, maintain, and retain, as determined by OHIP. The Contractor **MUST** provide Artifacts to OHIP upon request, or as otherwise directed, to support oversight, audits, and program needs.

The Contractor **MUST** produce and submit all applicable Deliverables and Artifacts identified in the format, structure, and cadence specified by OHIP or the Contract. OHIP may provide templates for the Contractor's use.

OHIP may modify the Deliverables and Artifacts required by this Appendix at any time to align with evolving program needs. Upon notice of changes, the Contractor **MUST** comply with all modifications and implement them promptly.

Table 10 – ITSM Standard Deliverables and Artifacts

Type	Name	Description
Deliverable	Business Continuity and Disaster Recovery Plan	The Contractor must develop a Business Continuity and Disaster Recovery (BC/DR) Plan to ensure the solution can continue operations during and after a significant disruption in business and/or technology operations. The plan must include, at a minimum, the following: • *Business Impact Analysis (BIA)* – Identification of the impact of disruptions on business operations, including critical systems and processes, Recovery Time Objectives (RTOs), and prioritization of restoration activities • *Risk Assessment* – Evaluation of potential threats (natural disasters, cyber-attacks, human error, technical failures), their likelihood and impact, and vulnerabilities within the systems • *Continuity and Recovery Strategies* – Strategies and solutions for maintaining business operations during disruptions and restoring hardware/infrastructure, applications, data, and connectivity, including both short-term and long-term recovery approaches • *Data Backup and Restoration Procedures* – Procedures for backing up critical data, including frequency, method, storage locations, and data restoration processes • *Roles, Responsibilities, and Emergency Contacts* – Identification of continuity and recovery team members, their roles and responsibilities, and comprehensive contact information for key personnel and emergency services • *Communication Plan* – Strategy for communicating with stakeholders during and after a disruption,

		including predefined templates and chain of command • *Training and Awareness Programs* – Materials and programs for training staff on their roles in BC/DR, including preparation to execute recovery plans • *Exercise and Testing Schedule* – Annual schedule and methodology for testing the plan, including tabletop exercises, simulation drills, and comprehensive recovery validation • *Maintenance and Review Schedule of the BC/BR Plan*– Schedule for regularly reviewing and updating the plan to ensure it remains current, including a change control process for incorporating updates • *Recovery Plan Documentation* – Step-by-step recovery plans for different disaster scenarios, including specific actions and criteria for returning to normal operations • *After-Action Report* – The approach to documenting lessons learned and recommendations for improvement following a disruption or drill. • *Assumptions, Constraints, and Dependencies* – Description of any assumptions, constraints, and dependencies that may impact BC/DR
Deliverable	Configuration Management Plan	The Contractor must develop a Configuration Management Plan that establishes the approach for identifying, controlling, tracking, and maintaining all configuration items throughout the solution life cycle, including infrastructure, software, documentation, and baselines. The Configuration Management Plan must include, at a minimum, the following: • *Configuration Item Identification* – Definition and classification of configuration items, including the scope of what is managed and the process for registering new Configuration Items • *Configuration Monitoring and Control* – How configuration will be tracked, managed, versioned, and controlled across all environments • *Configuration Management Artifacts* – Process for maintaining configuration records, baselines, and related documentation • *Configuration Audits* – Description of audits to verify that configuration records accurately reflect the deployed environment • *Reporting on Configuration Performance* – Description of audit results, configuration metrics, and compliance reporting • *Assumptions, Constraints, and Dependencies* – Description of any assumptions, constraints, and dependencies that may impact configuration management
Deliverable	Incident Management Plan	The Contractor must develop an Incident Management Plan that outlines the procedures and responsibilities for handling incidents that disrupt normal business operations or IT services. The Incident Management Plan must include, at a minimum, the following:

		• *Incident Life Cycle Procedures* – Documentation of the incident management policy, procedures, and workflows covering the full incident life cycle, including prioritization and escalation based on impact and urgency, investigation, diagnosis, resolution, and recovery, and post-incident review to identify root causes and implement corrective actions • *Roles and Responsibilities* – Matrix outlining the roles and responsibilities of all stakeholders involved in the incident management process • *Incident Logging and Classification* – Approach for logging and classifying incidents, ensuring consistent and accurate record-keeping • *Communication Plan* – Protocols for communicating incident status updates to relevant stakeholders, including users, support teams, and management • *Incident Reporting and Metrics* – Approach for generating reports and metrics on incident management performance, including KPIs such as mean time to resolve (MTTR) and incident volumes • *Training and Awareness* – Approach for training staff on incident management policies and procedures • *Continuous Improvement* – Strategy for ongoing monitoring and improvement of the incident management process • *Assumptions, Constraints, and Dependencies* – Description of any assumptions, constraints, and dependencies that may impact incident management
Deliverable	Maintenance and Operations (M&O) Plan	The Contractor must develop a Maintenance and Operations Plan that outlines the methodologies, processes, and schedules for managing day-to-day operations and must include, at a minimum, the following: • *Operational Framework Overview* – High-level summary of the methodologies and processes designed to ensure efficient and effective management of daily operations • *Maintenance Strategies* – Detailed information on maintenance approaches for infrastructure and software, focusing on ensuring system reliability and availability • *Roles and Responsibilities* – Specification of the roles and duties of the Contractor operations team, including responsibilities for maintaining operational efficiency • *Escalation Procedures* – Defined processes for escalating and addressing system issues and anomalies, ensuring timely resolution and minimal disruption • *System Reliability and Availability* – Methods and practices aimed at maintaining optimum system performance and minimizing downtime

		• *Review and Update Protocol* – Schedule for quarterly reviews or updates to the M&O Plan as needed to incorporate pertinent information or changes in operations • *Contact Information* – Details of who to contact for more information or to discuss any operational issues or changes outlined in the plan • *Assumptions, Constraints, and Dependencies* – Description of any assumptions, constraints, and dependencies that may impact M&O
Deliverable	Operations Report	The Contractor must develop an Operations Report that must include, at a minimum, the following: • *System Performance Metrics* – Measurements crucial for evaluating and planning capacity for system efficiency, reliability, and health, including, but not limited to, central processing unit (CPU) utilization, memory usage, storage operations, network throughput, response time, and service availability • *Program Support Metrics* – Measurements for assessing the effectiveness, efficiency, and overall support provided, which may include support and volume data that are specific to the program (e.g., applications processed, enrollment numbers, etc.) • *Production Defect Metrics* – Measurements that track defects identified in the production environment during M&O operations, including, but not limited to, the number of defects found, defect density, severity of defects, time to resolve them, and recurrence rate • *Special Provisions and SLA Metrics* – Provisions and metrics that include, but are not limited to, uptime, response and resolution times related to SLA, and SLAs compliance rates • *Daily Batch Operations* – Daily operations that include, but are not limited to, job completion time, success rate, failure rate, and time to recovery from errors • *Weekly Processing and Transaction Counts* – Data for all operational areas that includes, but is not limited to, the number of transactions processed, processing times, success rates, and error counts • *Staffing Contact Information Report* – Report that includes, but is not limited to, employee names, roles, phone numbers, email addresses, and emergency contacts • *Other Data* – Any other data required to perform statistical analysis required of each program by applicable state and federal agencies
Deliverable	Problem Management Plan	The Contractor must develop a Problem Management Plan that outlines the approach for identifying, analyzing, and resolving problems. It must include, at a minimum, the following: • *Problem Management Policy and Procedures* – Documentation of the principles, goals, roles,

		responsibilities, workflows, and communication protocols associated with problem management • *Problem Identification, Logging, and Categorization* – Methodology and procedures for identifying, logging, and categorizing problems • *Prioritization Methods* – Structured approach for prioritizing problems based on their impact and urgency • *Root Cause Analysis Approach* – Tools and methodologies for conducting root cause analysis to identify underlying causes of problems • *Problem Resolution Procedures* – Steps and actions for resolving problems, including approval processes, and the approach for capturing resolutions and workarounds for future use • *Reporting and Metrics* – KPIs and metrics to measure the effectiveness of problem management activities, including regular reports summarizing problem data, trends, and recurring issues • *Communication Plan* – How and when communication will occur with stakeholders, including notification of problem status, progress, and resolutions • *Training* – Approach for training relevant Contractor staff on problem management processes and tools • *ITSM Process Integration* – Approach for integrating problem management with other ITSM processes, such as incident management, change control, and configuration management • *Continuous Improvement* – Processes for ongoing assessment and enhancement of problem management practices • *Assumptions, Constraints, and Dependencies* – Description of any assumptions, constraints, and dependencies that may impact problem management
Deliverable	System Enhancement and Upgrade Report	The Contractor must develop a System Enhancement and Upgrade Report that provides a detailed assessment and overview of current system performance for any solution. The System Enhancement and Upgrade Report must include, at a minimum, the following: • *System Performance Overview* – A high-level summary of the current performance of the solution, identifying areas for improvement • *Areas for Improvement* – Analysis of specific areas where system efficiency, security, and functionality can be enhanced • *Proposed Enhancements and Upgrades* – Detailed description of proposed upgrades to software, infrastructure, and system functionalities to address identified areas for improvement • *Technical and Functional Aspects* – Comprehensive outline of the technical and functional specifications of the proposed enhancements, including integration details for new technologies

		• *Software Updates* – Information on software updates and how they will affect system operations and improve performance • *Infrastructure Updates* – Details on needed infrastructure upgrades to support new enhancements and optimize current system performance • *System Optimization Techniques* – Proposed techniques for optimizing system performance, ensuring long-term efficiency and reliability • *Integration of New Technologies* – Plans for incorporating new technologies to boost system capabilities and future-proof the infrastructure • *Recommendations and Action Items* – List of actions to be considered by the management team to implement proposed upgrades effectively
Deliverable	Training Plan	The Contractor must develop Training Plans that outline the key requirements essential for crafting a successful training program, including identifying the learning objectives, defining the target audience, and selecting appropriate training methods. A Training Plan must include, at a minimum, the following: • *Objectives* – Define clear, actionable goals that align with organizational objectives and skill competency • *Training Needs Assessment* – Describe how to determine the target audience, assess their knowledge and skills, and the approach to identifying the gaps between the audience capabilities and the knowledge and skills needed to use the system • *Audience Analysis* – Identify and describe user groups, including current skills, roles, and specific training needs • *Training Schedule* – Include a detailed timeline for when each training module will be delivered with session types, locations, equipment, and key milestones to assess progress and completion • *Training Methodologies* - Describe how the training will be conducted, considering various approaches (e.g. Instructor-led Training, Self-paced Learning, Hands-on Exercises, and interactive Elements) • *Instructional Materials* – Describe the approach to developing comprehensive resources tailored to system-specific operations such as manuals, tutorials, presentations and hands-on exercises • *Curriculum Content* – Outline the full training curriculum, including key topics, modules, learning objectives, user tasks, job aids, and troubleshooting guides • *Trainer Selection* – Determine essential qualifications and select trainers with years of experience in system functionalities and effective teaching skills.

		• *Delivery Methods* – Specify the mix of training formats (e.g., virtual, in-person, e-learning) to accommodate diverse learning styles • *Evaluation and Feedback Strategy* - Provide evaluation methods to measure the effectiveness of training sessions and implement processes for participants to provide feedback on training quality and relevance • *Communication Plan* – Outline how training information (e.g., registration, updates) will be communicated to participants • *Follow-up Support* – Describe any additional resources available such as online forums, help desks, or frequently asked questions for continued support • *Assumptions, Constraints, and Dependencies* – Description of any assumptions, constraints, and dependencies that may impact training
Deliverable	Transition-Out Execution	The Contractor must provide Transition-Out Execution, which serves as a collective set of activities performed by the Contractor to effectively implement the Transition-Out Plan, ensuring all outlined operations, services, and functions are addressed systematically. This deliverable facilitates project transparency and accountability by orchestrating the execution of tasks that align with strategic objectives defined within the Transition-Out Plan. It includes comprehensive coordination and management of resources and activities to achieve a seamless transition, adhering to established timelines and ensuring that all contractual requirements are met. The execution efforts are maintained in accordance with the preferred methods and practices to ensure successful implementation and integration.
Deliverable	Transition-Out Plan	The Contractor must develop a Transition-Out Plan that operationalizes the master Transition-Out Plan governed by the OHIP Program and Project Management Domain Document, Section 2.18 (Transition Management), outlining the comprehensive operational strategy and tasks necessary to successfully terminate the Contract and transfer the solution responsibilities. This plan must include, at a minimum, the following: • *Task and Deliverable Descriptions* – Detailed information on each task and deliverable required for the transition, ensuring clear understanding and execution • *Transition Scope Areas* – Coverage of all transition areas including Systems Administration (SA), Project Management (PM), Maintenance and Operations (M&O), and Design, Development, and Implementation (DDI) • *Detailed Schedule* – A timeline specifying the schedule for completing all tasks, including

		transitioning of system documentation, source code, and any in-flight system or application modifications • *Roles and Responsibilities* – Identification of roles and responsibilities to ensure accountability and smooth transition processes • *Training Plan* – A comprehensive plan for knowledge transfer, including the schedule of training sessions, site visits, and demonstrations; the number of staff to be trained; the training topics with objectives; and the length and location of each training session • *Status Reporting* – Summary of activities reported in Status Reports, ensuring consistent communication and monitoring of progress • *Approval* – Initiation of Transition-Out activities is contingent upon the request and approval • *Assumptions, Constraints, and Dependencies* – Description of any assumptions, constraints, and dependencies that may impact Transition-Out activities
Deliverable	Transition-Out Training and Knowledge Transfer Sessions	The Contractor must facilitate Transition-Out Training and Knowledge Transfer Sessions to describe the migration of knowledge and transfer of duties during the Transition-Out period. These sessions ensure that all aspects of Systems Administration (SA), Project Management (PM), Maintenance and Operations (M&O), and Design, Development, and Implementation (DDI) are effectively transferred. This deliverable facilitates project transparency and accountability by conducting structured sessions and demonstrations that showcase both logical and actual operations, verifying that Transition-Out activities are executed accurately and timely. The Contractor must establish and obtain acceptance for specific dates and times for these sessions and submit the content and format of the materials for review and approval prior to conducting them.
Artifact	Transition-Out Knowledge Transfer Artifacts	The Contractor must develop Knowledge Transfer Artifacts that serve as comprehensive tools for supporting the transfer of Maintenance and Operations (M&O) responsibilities of the solution during the Transition-Out period. These artifacts include all updated M&O manuals, documentation, training materials, demonstrations, and other relevant items.

Table 11 – Application Integration Deliverables and Artifacts

Type	Name	Description
Deliverable	Integration Technical Design Document (ITDD)	The Contractor must submit an Integration Technical Design Document (ITDD), which describes the design of all interfaces and processes involved in the integrations. Developed for integrations during the Design phase, the ITDD serves as a consolidated single point of reference for all integrations. It must include, at a minimum, the following: Overview of integration points and interfaces covered; Interface catalog listing the interfaces with their summary characteristics; Detailed technical design of each interface

		that enables the exchange of data with interface partner systems, documented in a separate Interface Control Document (ICD) for each interface; Batch control processes triggered by an interface, including the jobs' purpose and scope and the roles and responsibilities for all stakeholders, with a cross-reference to the System Architecture Design Document (the Technical Design Document) where full batch job detail is maintained; and a description of assumptions, constraints, and dependencies that may impact the ITDD. Batch jobs and batch processes not associated with an interface must be documented in the System Architecture Design Document (the Technical Design Document) in accordance with Section 8.4.2.2 (Solution Design). Batch coverage clarified (v5): interface-triggered batch processes remain documented in the ITDD with a cross-reference to the System Architecture Design Document, which serves as the authoritative home for all batch job documentation regardless of trigger.
Deliverable	Interface Control Document	The Contractor must submit an Interface Control Document (ICD), which serves as a detailed record and technical specifications of each interface/integration. It must include, but not be limited to: • Description of the interface/integration (e.g., federal, state, county, private entities) • Detailed interface/integration requirements • Interface/integration approach and processing involved • Communication protocols for the interface/integration • Endpoint configurations required to connect to partner system(s) • Orchestration details of the interface/integration • Interface/integration test schedule and cadence • Error handling

Table 12 – Infrastructure Management Standard Deliverables and Artifacts

Type	Name	Description
Deliverable	System Architecture Design Document (or equivalent)	The Contractor must develop a System Architecture Design Document (SADD) (or equivalent) that outlines the technical and architectural design of a system. It serves as a comprehensive blueprint that guides the planning, implementation, and management of the system architecture. The SADD must include detailed documentation, diagrams, and descriptions of the infrastructure, application components, security measures, network configurations, and change control processes. The SADD must include, at a minimum, the following: • *Executive Summary* – Provides an overview of the application and infrastructure, the purpose and objectives, and a summary of changes and design intentions • *Application and Infrastructure Architecture* – Details the overview of the supported application, including high-level architecture diagrams and descriptions of key components • *Infrastructure Details* – Includes detailed diagrams of current and proposed infrastructure, summarizing any changes or enhancements

		• *Compute and Storage Specifications* – Lists specifications of all servers, their roles, storage capacity, type, allocation details, and data retention and backup procedures • *Network Architecture and Configuration* – Outlines network topology, load balancers, routing, firewall configurations, IP address management, and subnetting details • *Security Design and Policies* – Describes firewall rules, security groups, network access control lists (NACLs), and authentication and encryption mechanisms • *Identity and Role Management* – Describes account types such as admin and service accounts, their permissions, and the implementation of role-based access controls • *Certificate and SMTP Management* – Lists all certificates, renewal and expiration management plans, and details of SMTP relay configuration and email policies • *Data Workflow Processes* – Provides detailed data flow diagrams, descriptions of data input, processing, and output, and key business and IT processes • *Change Control and Impact Analysis* – Details the change request process, documentation required for submission, review and approval pathways, impact analysis, risk assessments, and mitigation strategies • *Supporting Documentation and Appendices* – Includes detailed tables, charts, and additional diagrams

Table 13 – Ongoing Licensing and Support Standard Deliverables and Artifacts

Type	Name	Description
Deliverable	Procurement and Licensing Assessment Report	The Contractor must develop a Procurement and Licensing Assessment Report that provides an analysis of the usage and anticipated needs for products to inform their software procurement process for all components of the solution. At a minimum, the report must include, at a minimum, the following: • Expected and actual license usage metrics (as available) • Forecast of future licensing requirements based on system growth and evolving demands • Under/overutilization and optimization recommendations • Types of recommended licenses • Number of users/licenses required • Terms of use • License costs • Compliance considerations • Assessment of any unlimited license products requiring certification

		• Transparent reporting on license consumption and renewal timelines • Risk assessment for licenses approaching end-of-life or end-of-support • Comparison of current licensing model versus any proposed alternatives (e.g., subscription vs. perpetual)

Table 14 – Cloud FinOps Standard Deliverables and Artifacts

Type	Name	Description
Deliverable	Cloud FinOps Plan	The Contractor must develop a Cloud FinOps Plan to ensure the operation and costs of all cloud environments align with business goals, optimize performance, and ensure financial accountability. The Cloud FinOps Plan must include, at a minimum, the following: • *FinOps Governance and Operating Model* – Governance policies, decision-making structure, escalation paths, and alignment with business goals and regulatory requirements • *Roles and Responsibilities* – A detailed listing of all stakeholders involved, including their specific roles, responsibilities, and authority levels • *Financial Management Practices* – Approach to budgeting, cost allocation, cost forecasting, and solution value tracking • *Cost Optimization and Efficiency* – Resource and capacity management, optimization techniques, and cost monitoring and alerting • *Assumptions, Constraints, and Dependencies* – Description of any assumptions, constraints, and dependencies that may impact Cloud FinOps
Deliverable	Monthly Cloud Usage and Spend Report	The Contractor must develop a Monthly Cloud Usage and Spend Report that provides insight into how cloud resources are being utilized, their efficiency, and their overall cost impact. This report must include cloud usage and spend in various ways to inform the outcome of the resources rightsizing process. The Monthly Cloud Usage and Spend Report must include, at a minimum, the following: • *Usage Statistics* – Summarizes cloud resource consumption, including compute, storage, networking, and service usage, across environments and time periods • *Performance Metrics* – Provides key indicators of system performance and reliability, such as availability, latency, throughput, and resource utilization trends • *Cost Analysis* – Breaks down cloud spending by service, environment, application, or business unit, and identifies cost drivers, anomalies, and areas of increased spend • *Resource Efficiency* – Assesses how effectively cloud resources are sized and utilized, highlighting

Type	Name	Description
		underutilized, overprovisioned, or idle resources for optimization • *Resource Provisioning and De-Provisioning* – Describes how cloud resources are provisioned and deprovisioned, including automation practices, approval processes, and life cycle management • *Future Projections* – Forecasts expected cloud usage and costs based on historical trends, planned initiatives, and anticipated changes in demand • *Strategy Adjustments* – Recommends actions and strategy changes to improve cost efficiency, performance, governance, or alignment with organizational objectives

Appendix B: Master Requirements Summary

The following table consolidates all 249 requirements from this domain standard with individual RFC 2119.

Table 15 – Master Requirements Summary Table

Req. ID	Requirement Statement	Tier	Standard Section
Section 2.0—ITSM Standard | INFRA-0001 to INFRA-0059 | 59 Requirements: MUST 58 | SHOULD 0 | MAY 1			
INFRA-**0001**	Adhere to integration principles: seamless service delivery across vendor boundaries, transparent hand-offs, coordinated incident/problem management, unified reporting, and consistent change management.	**MUST**	2.9.1—Integration Principles
INFRA-**0002**	Map internal roles to the OHIP and State Enterprise role framework. Designate named individuals for each required role and provide assignments to OHIP during onboarding. Communicate role changes within five business days.	**MUST**	2.9.2—OHIP and Contractor Responsibilities
INFRA-**0003**	For systems classified as Critical, ensure 24/7 coverage for the Incident Manager role.	**MUST**	2.9.2—OHIP and Contractor Responsibilities
INFRA-**0004**	Support integration with OHIP's ITSM Solution as specified in individual contracts and integration agreements.	**MUST**	2.9.3—Integration with OHIP's ITSM Solution
INFRA-**0005**	Record external ticket references (system name, ticket ID, status, contact name) in designated custom fields. Maintain all communications in ticket comments for audit trail.	**MUST**	2.9.3—Cross-System Ticket Dependencies
INFRA-**0006**	Update ticket status to Pending External Resolution when blocked by external dependency. Set follow-up reminders per incident priority. Document all status updates from external systems.	**MUST**	2.9.3—Status Management
INFRA-**0007**	Escalate to OHIP System Manager if external ticket shows no progress: Priority 1 within 2 hours, Priority 2 within 4 hours, Priority 3 within 1 business day.	**MUST**	2.9.3—Escalation Protocol
INFRA-**0008**	OHIP ticket cannot be closed until external dependency is resolved or workaround documented. Final documentation **MUST** include resolution summary and lessons learned.	**MUST**	2.9.3—Resolution Requirements
INFRA-**0009**	Operating external ITSM platforms **MUST** establish integration with OHIP's ITSM solution using approved patterns (API, Webhook, Scheduled Sync, or Manual Cross-Reference).	**MUST**	2.9.3—Integration Standards
INFRA-**0010**	Consult OHIP Technology Leadership regarding applicable reference integration models for new vendor integrations.	**MUST**	2.9.3—Reference Integration Models
INFRA-**0011**	All involved vendors **MUST** respond within escalation timeframes per SLAs. Status updates **MUST** be posted to shared ticket at intervals appropriate to priority. All related vendor tickets **MUST** be linked in OHIP's ITSM solution.	**MUST**	2.9.4—Cross-Solution Issue Management
INFRA-**0012**	Establish escalation paths enabling timely resolution at each support tier (L1→L2→L3→executive). Ensure internal processes support contracted service levels.	**MUST**	2.9.5—Escalation Procedures
INFRA-**0013**	For Priority 1 incidents, establish or join conference bridge within 15 minutes. For Priority 2 with cross-vendor impact,	**SHOULD**	2.9.5—Major Incident Conference Bridge

	within 30 minutes. Required participants **MUST** include Incident Manager and OHIP System Manager.		
INFRA-**0014**	During active Priority 1 incidents, provide status updates every 30 minutes. For Priority 2, every 60 minutes. All updates **MUST** be posted to the ticket.	**SHOULD**	2.9.5—Communication Cadence
INFRA-**0015**	Escalate to OHIP Technology Leadership if incident not contained within 1 hour of bridge activation. Escalate to vendor management if no resolution path within 2 hours (P1) or 4 hours (P2).	**SHOULD**	2.9.5—Escalation Triggers
INFRA-**0016**	Implement general management practices in accordance with OHIP requirements.	**MUST**	2.4—General Management Practices
INFRA-**0017**	Align practices and services with changing business needs through ongoing improvement. Execute the seven steps of Continual Improvement. Capture data and present analysis per agreed cadence.	**SHOULD**	2.4.1—Continual Improvement
INFRA-**0018**	Protect information through security controls commensurate with risk. Ensure confidentiality, integrity, and availability compliance. Implement administrative, physical, and technical security controls.	**MUST**	2.4.2—Information Security Management
INFRA-**0019**	Establish and maintain effective relationships with OHIP stakeholders through regular communication, engagement activities, and proactive issue resolution.	**MUST**	2.4.3—Relationship Management
INFRA-**0020**	Ensure suppliers and their performance are managed appropriately. Report SLA breaches to the OHIP Contract Management team.	**MUST**	2.4.4—Supplier Management
INFRA-**0021**	Create Training Plans, training artifacts, and SOPs stored in OHIP's ITSM Knowledge Repository. Improve effective use of knowledge across the organization.	**SHOULD**	2.4.5—Knowledge Management
INFRA-**0022**	Enable effective change adoption through people-focused approaches. Support OHIP's OCM initiatives with clear communication, training, and feedback.	**MUST**	2.4.6—Organizational Change Management
INFRA-**0023**	Adhere to OHIP's Project Management Standard for all approved projects and initiatives, providing status reports, managing risks, and meeting deliverable criteria.	**SHOULD**	2.4.7—Project Management
INFRA-**0024**	Identify, assess, and control risks related to solution or services. Coordinate with OHIP and stakeholders to mitigate identified risks.	**MUST**	2.4.8—Risk Management
INFRA-**0025**	Ensure financial resources are used effectively. Provide financial information to support OHIP's cost tracking and charge-back/show-back models.	**MUST**	2.4.9—Service Financial Management
INFRA-**0026**	Understand OHIP's strategic goals and ensure services and improvement initiatives are aligned with that strategy.	**SHOULD**	2.4.10—Strategy Management
INFRA-**0027**	Provide OHIP with accurate service portfolio information including performance, costs, and dependencies.	**SHOULD**	2.4.11—Portfolio Management
INFRA-**0028**	Adhere to OHIP's Enterprise Architecture Standards and approved Configuration Management Plan. Seek OHIP approval for all architectural decisions through the OHIP EA governance process.	**MUST**	2.4.12—Architecture Management
INFRA-**0029**	Measure, monitor, and report on service performance as defined in this standard and contracts. Provide accurate and timely reports in OHIP-specified format.	**MUST**	2.4.13—Measurement and Reporting

INFRA-**0030**	Ensure staff are appropriately qualified and trained. Fill roles per Section 2.7; roles **MAY** be combined with OHIP approval based on contract size and complexity.	**SHOULD**	2.4.14—Workforce and Talent Management
INFRA-**0031**	Ensure services deliver agreed levels of availability to meet customer and user needs. Establish mechanisms to capture and report agreed-upon capacity and performance metrics to the Department per contractual agreements. Maintain the M&O Plan; maintain software at the N-1 version level.	**MUST**	2.5.1—Availability Management
INFRA-**0032**	Participate in business analysis activities, providing technical and domain expertise to define requirements and evaluate solutions.	**MUST**	2.5.2—Business Analysis
INFRA-**0033**	Ensure services achieve agreed performance levels. Execute performance, stress, and load testing. Make necessary modifications to achieve acceptable production performance levels.	**MUST**	2.5.3—Capacity and Performance Management
INFRA-**0034**	Establish and document the approaches and processes for managing service and product changes, maximizing successful changes by assessing risks, authorizing changes, and managing the change schedule. Initiate Technical Change Requests in OHIP's solution with 10-day minimum lead time for normal changes.	**MUST**	2.5.4—Change Enablement
INFRA-**0035**	Perform post-implementation test on each change to verify security features and boundaries are unchanged.	**MUST**	2.5.4—Change Enablement
INFRA-**0036**	Minimize incident impact by restoring normal service operation as quickly as possible. Manage all incidents using an OHIP-approved Incident Management Plan.	**MUST**	2.5.5—Incident Management
INFRA-**0037**	Plan and manage the full life cycle of all IT assets. Maintain accurate records of asset location, ownership, and status. Manage software license compliance. Retain configuration change records for at least 3 years.	**MUST**	2.5.6—IT Asset Management
INFRA-**0038**	Systematically observe services and components. Perform event detection, logging, categorization, correlation, prioritization, escalation, resolution, and closure. Maximize automation.	**MUST**	2.5.7—Monitoring and Event Management
INFRA-**0039**	Reduce incident likelihood by identifying actual and potential causes. Detail processes in the Problem Management Plan.	**MUST**	2.5.8—Problem Management
INFRA-**0040**	Manage the entire Release and Deployment Management life cycle. Utilize static and dynamic code scan software before production Release. Make scan reports and performance test results available to OHIP before every production Release.	**MUST**	2.5.9—Release Management
INFRA-**0041**	Serve as a single source of consistent information on all services. Provide and update a Service Catalog with accurate details on status, interactions, and dependencies.	**MUST**	2.5.10—Service Catalog Management
INFRA-**0042**	Ensure accurate configuration information is available when needed. Create and execute an approved Configuration Management Plan. Maintain a CMDB supporting Incident, Problem, and Change Control. Maintain older baseline configurations for rollback.	**MUST**	2.5.11—Service Configuration Management
INFRA-**0043**	Ensure availability and performance are maintained in the event of a disaster. Develop the BC/DR Plan based on Enterprise requirements.	**MUST**	2.5.12—Service Continuity Management

INFRA-**0044**	Design products and services fit for purpose, fit for use, and deliverable by the organization. Work with OHIP Technology leadership to ensure design activities are documented, controlled, and aligned with business strategy.	**MUST**	2.5.13—Service Design
INFRA-**0045**	Capture demand for incident resolution and service requests. Establish a Service Desk as the single point of contact for users.	**MUST**	2.5.14—Service Desk
INFRA-**0046**	Establish, monitor, and report on service levels using Service Level Agreements per OHIP's Service Level Management framework.	**MUST**	2.5.16—Service Level Management
INFRA-**0047**	Handle all pre-defined service requests in an effective manner. Triage, accept, or transfer requests using the change enablement process per the M&O Plan. Emphasize self-service capabilities.	**MUST**	2.5.17—Service Request Management
INFRA-**0048**	Ensure new or changed services meet defined requirements before deployment. Perform post-implementation testing of all changes to verify functionality and security boundaries. Update Change Requests in OHIP's solution to verify testing completion.	**MUST**	2.5.18—Service Validation and Testing
INFRA-**0049**	Execute deployment activities including planning, scheduling, execution, and early life support. Provide deployment runbooks and rollback procedures to OHIP.	**MUST**	2.6.1—Deployment Management
INFRA-**0050**	Support Transition-Out phase to OHIP or Successor Contractor. Begin Transition-Out only after OHIP approval. Ensure uninterrupted services including complete data transfer. Develop a Transition-Out Schedule.	**MUST**	2.6.1—Deployment Management (Transition)
INFRA-**0051**	Oversee infrastructure and platforms including server, network, storage, middleware, and database management per OHIP performance standards.	**MUST**	2.6.2—Infrastructure and Platform Management
INFRA-**0052**	Ensure applications meet stakeholder needs in functionality, reliability, maintainability, compliance, and auditability. Follow OHIP SDLC Standard. Meet code quality, testing, and security scanning requirements before production release.	**MUST**	2.6.3—Solution Development and Management
INFRA-**0053**	Fill management roles (System Manager, Service Desk, M&O, Change Enablement, Release/Deployment, Application/Technical, IT Operations) with qualified staff. Roles **MAY** be combined with OHIP approval.	**MUST**	2.7—Management Roles
INFRA-**0054**	System Manager **MUST** perform minimum responsibilities including capacity/availability/performance management, capacity planning, SLA compliance, availability reporting, and demand estimation.	**SHOULD**	2.7.1—System Manager Role
INFRA-**0055**	L1 Service Desk **MUST** provide first point-of-contact support. L0 self-service **MUST** handle initial support. Escalation to L2 **MUST** be seamless.	**MUST**	2.7.2—Service Desk Roles
INFRA-**0056**	Fill Change Enablement roles: Change Manager, Change Member, Risk Evaluation Manager, and Configuration/Asset Manager. Configuration/Asset Manager **MUST** perform periodic CMDB audits.	**SHOULD**	2.7.4—Change Enablement Supporting Roles
INFRA-**0057**	Leverage industry-standard tools providing required service management core capabilities (incident, request, problem, change, release, asset/config, knowledge management).	**MUST**	2.8—ITSM Tools and Technology

INFRA-**0058**	The Contractor **MAY** use their existing ITSM tools provided they meet capability requirements, support OHIP integration, provide required reporting, and support future enterprise tooling transition.	**MAY**	2.8—ITSM Tools and Technology
INFRA-**0059**	Maintain compatibility with OHIP Preferred Operational Tools Standard. Participate in tool standardization initiatives. Support data migration to enterprise tools when required. Provide tool training and knowledge transfer.	**SHOULD**	2.8—ITSM Tools and Technology
Section 3.0—Application Integration Standard | ARCH-0001 to ARCH-0050 | 50 Requirements: MUST 44 | SHOULD 6 | MAY 0			
ARCH-**0001**	Comply with both this Enterprise Application Integration Standard and the OHIP Secure API Development Baseline requirements.	**MUST**	3.3—Integration Governance (Companion Standard)
ARCH-**0002**	Submit integration plans and designs to OHIP for review and approval to ensure conformance with this standard and relevant federal/industry standards before implementation.	**MUST**	3.3—Integration Compliance Review
ARCH-**0003**	Ensure all inbound interfaces for new OHIP systems utilize HTTPS. Exceptions for any protocol other than HTTPS (e.g., FTPS, SFTP, SCP) **MUST** be granted by OHIP.	**MUST**	3.3—HTTPS Inbound
ARCH-**0004**	Ensure all exposed APIs are published through an OHIP-approved API gateway, which **MUST** serve as the single-entry point enforcing policies (routing, throttling, authentication, inspection, encryption, metadata, monitoring) for all API traffic.	**MUST**	3.3—API Gateway
ARCH-**0005**	If unable to use OHIP's preferred API gateway, provide explanation for OHIP approval. Alternate gateways **MUST** provide API lifecycle management, monitoring, securing, documenting, and comply with resiliency and performance requirements.	**MUST**	3.3—API Gateway
ARCH-**0006**	Ensure the API gateway enforces authentication for both end-user and service-to-service calls, applying consistent security controls across all integrations.	**MUST**	3.3—Policy Enforcement
ARCH-**0007**	Ensure all integration interfaces (APIs, message feeds, file transfer endpoints) are registered in a catalog with designated owners, version, contact, performance info, availability SLAs, and usage policies. All new interfaces **MUST** be documented and modeled in OHIP's Enterprise Architecture tool.	**MUST**	3.3—Registry and Ownership
ARCH-**0008**	Before creating new interfaces, search OHIP registries to identify opportunities to re-use existing services/interfaces.	**MUST**	3.3—Registry and Ownership
ARCH-**0009**	Use nationally recognized data exchange standards per CMS requirements in all integrations, including HIPAA-adopted transaction standards (ASC X12N EDI), ACA, CMS, and ONC interoperability standards.	**MUST**	3.4.1—Adoption of Industry Standards
ARCH-**0010**	For clinical or public health data exchange, support the latest release version of HL7 messaging. Messages **MUST** follow HL7 v2 (or later) defined profiles for structure and content.	**MUST**	3.4.1—HL7 Messaging
ARCH-**0011**	Ensure all new application integrations exposing health data implement HL7 FHIR R4 (or later) for RESTful APIs using standard FHIR resources and profiles (e.g., US Core).	**MUST**	3.4.1—FHIR APIs

ARCH-**0012**	Ensure Medicaid administrative data exchanges use ASC X12N or later EDI formats as mandated by HIPAA. All required transactions **MUST** adhere to X12 Implementation Guides for content and code sets.	**MUST**	3.4.1—X12 EDI Transactions
ARCH-**0013**	For non-healthcare integrations, APIs **MUST** implement RESTful design principles, publish definitions using OpenAPI specifications, and exchange data using structured machine-readable formats (e.g., JSON) with OHIP-approved schemas.	**MUST**	3.4.1—General Web and RESTful API Standards
ARCH-**0014**	Non-standard or proprietary interfaces are not allowed unless an exception is approved and documented.	**MUST**	3.4.1—General Web and RESTful API Standards
ARCH-**0015**	For real-time, highly scalable, loosely coupled scenarios, utilize asynchronous event-driven architecture (EDA). EDA patterns **MUST** provide loose coupling so a producing system can publish events without direct dependencies on consuming systems' availability; consuming systems are responsible for reacting to events per their own processing and availability requirements.	**MUST**	3.4.2—Event-Driven Architecture
ARCH-**0016**	Event-driven patterns **MUST** utilize standard protocols (e.g., AMQP 1.0, JMS, MQTT) and standardized frameworks for event payload structure and metadata (e.g., CloudEvents).	**SHOULD**	3.4.2—Event-Driven Architecture
ARCH-**0017**	All event topics, queues, and subscriptions **MUST** be registered in an OHIP-approved event catalog with defined ownership, description, and data contracts.	**MUST**	3.4.2—Event-Driven Architecture
ARCH-**0018**	Ensure all events adhere to OHIP-approved standardized event structures including common headers, metadata, and data schemas. Maintain a central event catalog and taxonomy.	**MUST**	3.4.2—Standardization of Event Structures
ARCH-**0019**	Enforce schema evolution policies to ensure backward and forward compatibility and prevent breaking changes for downstream consumers.	**MUST**	3.4.2—Standardization of Event Structures
ARCH-**0020**	Use push-based event notification mechanisms (e.g., webhooks) where immediate change notification is required. Pull mechanisms (e.g., scheduled polling) are permitted only where push is impractical.	**SHOULD**	3.4.2—Push-Pull Mechanisms
ARCH-**0021**	Document and review approved use cases and integration patterns for both push and pull mechanisms.	**MUST**	3.4.2—Push-Pull Mechanisms
ARCH-**0022**	Utilize dedicated streaming platforms for continuous, high-volume data flows. Ensure efficient ingestion, processing, and distribution with scalability and fault tolerance.	**MUST**	3.4.2—Data Streaming
ARCH-**0023**	Monitor data streams with retention and replay capabilities. Version and manage schemas using a centralized schema registry enforcing evolution policies.	**MUST**	3.4.2—Data Streaming
ARCH-**0024**	For API (RESTful/FHIR) integrations: comply with NIST SP 800-228, use JSON/XML payloads conforming to FHIR schemas, support RESTful operations with consistent URIs, and use an OHIP-approved API Gateway.	**MUST**	3.4.3—Integration Protocol—API
ARCH-**0025**	For EDI (X12) transactions: use ASC X12N standards, HTTPS for inbound EDI, secure channels for transmission, and ensure acknowledgment/response mechanisms are in place.	**MUST**	3.4.3—Integration Protocol—EDI

ARCH-**0026**	For outbound file transfers: use secure protocols, encrypt sensitive data in transit and at rest, automatically scan all files for malware, quarantine failures, log to SIEM, update threat definitions daily, and use an OHIP-approved managed file transfer solution.	**MUST**	3.4.3—Integration Protocol—File Transfer
ARCH-**0027**	For event-driven messaging: employ publish/subscribe or message queue patterns, limit event messages to 256KB (larger via API), use a messaging broker with reliable delivery, design idempotent messages, and route through an OHIP-approved event/message broker.	**SHOULD**	3.4.3—Integration Protocol—Event-Driven
ARCH-**0028**	For any batch file exchange, return an acknowledgement to the sending system confirming receipt and processing outcome (e.g., accepted, accepted with errors, rejected). An exception **MAY** be granted through the SDR process (Section 1.7.1) where the batch file is a one-way distribution and non-transactional.	**SHOULD**	3.4.3—Integration Protocol—Event-Driven
ARCH-**0029**	Produce detailed logs accessible by OHIP for all integrations. Log every transaction, message transfer, source IP, timestamps, source/destination, and outcome. Follow OWASP logging cheat sheet. Logs **MUST** be accessible with an OHIP-approved analysis tool.	**SHOULD**	3.5—Logging and Audit Trails
ARCH-**0030**	Implement continuous monitoring of integration workflows tracking throughput, latency, and error rates. Set up automated alerts for failures, anomalies, or SLA breaches. Automatically create incidents as agreed with the Department.	**MUST**	3.5—Monitoring and Alerts
ARCH-**0031**	Validate data content and format against schemas or implementation guides at integration endpoints. Reject invalid or non-conforming messages with error notifications.	**MUST**	3.5—Data Validation
ARCH-**0032**	Backward-incompatible changes to existing integration interface versions are not allowed unless an exception is approved and documented. Changes require a new version rather than breaking existing contracts.	**MUST**	3.6—Version Control
ARCH-**0033**	Proposed integration changes **MUST** go through a formal change control process. Changes **MUST** be documented and approved by OHIP before implementation. Emergency changes require retrospective review.	**MUST**	3.6—Change Approval
ARCH-**0034**	Every integration change request **MUST** include an impact analysis covering affected systems, data impacted, and compliance review.	**MUST**	3.6—Impact Analysis
ARCH-**0035**	Coordinate changes with all stakeholders. Notify external partners/agencies well in advance. Provide testing opportunities; OHIP **MUST** approve testing opportunities and results.	**MUST**	3.6—Partner Coordination
ARCH-**0036**	Update integration documentation and catalogs as part of every change rollout, including API specifications, interface control documents, and release notes.	**MUST**	3.6—Documentation Updates
ARCH-**0037**	Validate all integrations for compliance with relevant standards during development and prior to Go-Live (e.g., HL7/FHIR validators, X12 EDI syntax checkers).	**MUST**	3.7—Standards Compliance Testing
ARCH-**0038**	Provide non-production test endpoints for integration testing by external applications. Test endpoints **MUST** mirror production APIs including versioning consistency, provide robust security, access non-production	**MUST**	3.7—Test Endpoints

	environments, provide secure data stores, support data reset, provide realistic data, include developer documentation, and use only test credentials.		
ARCH-**0039**	Handle errors gracefully without data loss. Sanitize error messages returned to users/partners; capture technical details in internal logs.	**MUST**	3.8—Graceful Error Handling
ARCH-**0040**	Implement retry mechanisms for transient failures with bounded back-off to avoid infinite loops.	**MUST**	3.8—Retry and Recovery
ARCH-**0041**	Design integrations to be idempotent so retrying does not create duplicate transactions.	**MUST**	3.8—Idempotency
ARCH-**0042**	Use resilience techniques including load balancing and circuit breakers to avoid single points of failure. Circuit breakers **MUST** trigger fallback logic (e.g., queuing for later processing).	**MUST**	3.8—Resilience Patterns
ARCH-**0043**	Critical integration components **MUST** have high-availability and failover plans. Implement clustering or backups for message queues and integration runtimes. Ensure files are not lost if transfer is interrupted.	**MUST**	3.8—Failover and Continuity
ARCH-**0044**	Establish automated alerts for integration errors. Notify responsible teams in real time. Monitor dead-letter queues daily. Track all unresolved errors to closure via incident management.	**SHOULD**	3.8—Error Notification
ARCH-**0045**	Provide comprehensive documentation for all integration interfaces including API specifications (OpenAPI/Swagger), data models, sample requests/responses, message schemas, and EDI companion guides. Keep documentation up to date and accessible.	**MUST**	3.9—Interface Specifications
ARCH-**0046**	Host API definitions in a Central API Catalog for discovery. Include metadata tags (data domain, owning team, compliance category) to facilitate search and governance.	**MUST**	3.9—Central API Catalog
ARCH-**0047**	Provide test endpoints, example clients, authorization requirements, and sample credential setup for APIs. Indicate a support contact or forum in documentation for issue resolution and onboarding.	**MUST**	3.9—Developer Support
ARCH-**0048**	Treat documentation as a required deliverable for any new integration or change. Integration points are considered incomplete until documentation and discoverability requirements are met in full.	**MUST**	3.9—Document Maintenance
ARCH-**0049**	Produce and submit all Deliverables identified in Appendix A in the format, structure, and cadence specified by OHIP.	**MUST**	Appendix A—Deliverables and Artifacts
ARCH-**0050**	Upon notice of modifications to Appendix A, comply with all updated deliverable and artifact requirements.	**MUST**	Appendix A—Deliverables and Artifacts
Section 4.0—Infrastructure Management Standard | INFRA-0060 to INFRA-0094 | 35 Requirements: MUST 35 | SHOULD 0 | MAY 0			
INFRA-**0060**	Implement a cloud-hosted delivery model with SaaS as the preferred service model. Host Enterprise Cloud Solutions on infrastructure maintained by personnel in the continental United States.	**MUST**	4.3—OHIP Infrastructure Management Strategy
INFRA-**0061**	Ensure the solution resides in a cloud environment complying with FedRAMP Moderate or higher, ARC-AMPE, SSA requirements, and OHIP-specific requirements.	**MUST**	4.3—OHIP Infrastructure Management Strategy

INFRA-**0062**	Utilize the security framework in the OHIP Security and Privacy Compliance Standard for infrastructure and managed services. Submit exception requests for OHIP review and approval.	**MUST**	4.3—OHIP Infrastructure Management Strategy
INFRA-**0063**	Provide support for PaaS and IaaS service models as needed. All cloud environment ownership **MUST** belong to OHIP.	**MUST**	4.3—OHIP Infrastructure Management Strategy
INFRA-**0064**	Provide infrastructure solutions using Cloud Service Provider models (SaaS, PaaS, IaaS). Recommend specific PaaS types for OHIP evaluation and approval.	**MUST**	4.4.1—Infrastructure Services and Solution Models
INFRA-**0065**	Provide detailed infrastructure documentation and specifications for OHIP to assess service levels, security measures, and identify risks.	**MUST**	4.5.2—Infrastructure Management Functions
INFRA-**0066**	Provide OHIP with usage/cost of each cloud component broken down by account/subscriptions. Perform periodic usage analytics and make available to OHIP. Comply with the OHIP Cloud FinOps Standard.	**MUST**	4.5—SaaS Cost Management
INFRA-**0067**	Comply with all requirements of the OHIP Security and Privacy Compliance Standard, including hosting, data loss protection, threat protection, and vulnerability reporting.	**MUST**	4.5—SaaS Security and Privacy
INFRA-**0068**	Collaborate with OHIP for data usage approvals; maintain audit logs of data access; comply with OHIP data governance policies; provide data management practices for OHIP review.	**MUST**	4.5—SaaS Data Management
INFRA-**0069**	Review and seek approval of infrastructure architecture through OHIP review process. Maintain a Bill of Materials for cloud services. Adhere to OHIP Enterprise monitoring tool standards.	**MUST**	4.5—SaaS Infrastructure Automation
INFRA-**0070**	Obtain OHIP review and approval for: infrastructure architecture, all cloud services and software, and any major changes before production usage.	**MUST**	4.5—SaaS Infrastructure Automation
INFRA-**0071**	Collaborate with OHIP to develop and maintain Service Level Agreements.	**MUST**	4.5—SaaS Performance Management
INFRA-**0072**	Comply with the OHIP Cloud FinOps Standard. Obtain OHIP approval for all costs incurred for storage, computing, and cloud resources, and for monthly budgets by cloud component.	**SHOULD**	4.5—P/IaaS Cost Management
INFRA-**0073**	Comply with all SaaS infrastructure automation requirements. Submit Cloud Design Document or SADD for OHIP approval before implementation. Implement CI/CD pipeline. Work with OHIP to reduce legacy footprints.	**SHOULD**	4.5—P/IaaS Infrastructure Automation
INFRA-**0074**	Obtain OHIP review and approval for all architecture, design, implementation, containerization, and CI/CD pipeline for releases.	**MUST**	4.5—P/IaaS Infrastructure Automation
INFRA-**0075**	Provide minimum environments: DEV, Data Conversion, TEST/SIT, UAT/Stage, Performance, PRE-PROD, PROD, and DR. Comply with specified requirements for each environment per the environments table.	**MUST**	4.6.1—Environments

INFRA-**0076**	Document a comprehensive BC/DR Plan for all production solutions, approved by OHIP. Perform DR Test before go-live and annually. Submit DR test results within two weeks.	**MUST**	4.6.1—Business Continuity and DR
INFRA-**0077**	Ensure production changes supporting BC/DR are deployed using the OHIP Release Management Standard and approved via the OHIP Technical Change Control Standard. Submit BC/DR architecture and test evidence through OHIP architecture review.	**MUST**	4.6.1—Business Continuity and DR
INFRA-**0078**	Refer to the OHIP Preferred Operational Tools Standard before proposals or procurements. Obtain OHIP approval for any technology modifications or software installation. Maintain all solutions at n-1 version level.	**SHOULD**	4.7—Technology Standards
INFRA-**0079**	Provide OHIP with complete visibility and administrative access to OHIP-owned cloud resources. Track and report application performance. Define ownership of each cloud component's support accountabilities.	**MUST**	4.8—Operational Standards
INFRA-**0080**	Follow the OHIP Technical Change Control Standard for all infrastructure/platform changes. Follow the OHIP Program and Project Management Domain Document, Project Change Control Standard for scope/schedule/funding changes. No production change without an approved change record.	**MUST**	4.9.1—Change Control
INFRA-**0081**	Log change requests prior to implementation with required lead times. Include impact analysis and architecture review approvals for cross-solution changes. Patches/upgrades **MUST** follow an approved Patch Management Plan.	**MUST**	4.9.1—Change Control
INFRA-**0082**	Document and report all storage usage to OHIP monthly including utilization details, storage types, burn rates, hosting entities, and storage eligible for release. Provide storage forecasts at OHIP-determined frequency (not exceeding annually).	**SHOULD**	4.9.2—Storage Management
INFRA-**0083**	Build all core infrastructure to provide minimum 99.99% availability. Design cloud solutions to meet agreed availability requirements utilizing cloud redundancy features. Implement geo-redundancy as necessary.	**SHOULD**	4.9.3—Availability and Recoverability
INFRA-**0084**	Perform daily full backups and weekly full database backups with daily incremental backups as minimum. Provide evidence of completion; investigate and re-run failed backups daily.	**MUST**	4.9.4—Backup Management
INFRA-**0085**	Retain backups per OHIP retention requirements. Document, review, and obtain OHIP approval for backup schedule, frequency, and retention policy. Regularly validate backups. Ensure backups conform to data residency requirements.	**MUST**	4.9.4—Backup Management
INFRA-**0086**	Ensure cloud solutions are interoperable with OHIP toolsets, alerting processes, and monitoring expectations. Maintain host details in OHIP CMDB. Produce raw vulnerability and compliance scan results in shareable formats.	**MUST**	4.10—Monitoring and Optimization
INFRA-**0087**	Provide configurable alerting mechanism for infrastructure, applications, and services. Provide analytical and operational reporting interoperable with OHIP Enterprise Solution. Monitor all infrastructure components with itemized cost allocations.	**MUST**	4.10—Monitoring and Optimization

INFRA-**0088**	Design cloud solutions using resilience-leading practices to protect against DDoS, spoofing, man-in-the-middle, and other threats.	**MUST**	4.10—Monitoring and Optimization
INFRA-**0089**	Track all incidents and events comprehensively. Report solution outages as incidents in OHIP's tracking solution. Ensure enterprise monitoring integrations auto-generate incident records in OHIP's ITSM tooling.	**MUST**	4.11—Incident and Event Management
INFRA-**0090**	Ensure cloud solutions are interoperable with OHIP enterprise tools including FIM, SOC, and SIEM.	**MUST**	4.11—Incident and Event Management
INFRA-**0091**	Monitor, scale, document, and report performance metrics per OHIP standards. Measure performance using OHIP's five categories: User Interface, Application Response Time, Real-Time Interfaces, Data Queries, and Image Response Time.	**MUST**	4.12—Performance Standards
INFRA-**0092**	Adhere to operational performance measurement and reporting requirements, providing data elements per Table 5 for each of OHIP's five performance categories.	**MUST**	4.13—Operational Performance Measurement
INFRA-**0093**	Ensure all solutions are continuously monitored. Implement collaborative performance baselining, monitoring, reporting, and alerts. Establish processes for detecting and resolving performance degradation.	**MUST**	4.14—Operational Performance Monitoring
INFRA-**0094**	Scan inbound and outbound data traffic for reputation, malware, spam, and other criteria defined by OHIP.	**MUST**	4.14—Operational Performance Monitoring
Section 5.0—Log Management Standard | INFRA-0095 to INFRA-0120 | 26 Requirements: MUST 26 | SHOULD 0 | MAY 0			
INFRA-**0095**	Support OHIP in the timely identification, search, retrieval, analysis, and presentation of log data related to MES operations when required for audits, investigations, oversight, litigation, or other legal or regulatory matters.	**MUST**	5.3—OHIP Logging Governance
INFRA-**0096**	Preserve log integrity, maintain chain-of-custody where applicable, and ensure requested information is provided within the timeframe specified by OHIP.	**MUST**	5.3—OHIP Logging Governance
INFRA-**0097**	Ensure all OHIP MES systems generate logs for security-relevant and business-critical events, including but not limited to: authentication, privileged access, data access (PHI/PII/FTI), business transactions, and configuration changes.	**MUST**	5.3—Audit Events Record Generation
INFRA-**0098**	Ensure all authentication success/failure attempts are recorded with the log fields specified in Table 24 (user ID, authentication method, timestamp, source IP/device, target system, result).	**MUST**	5.3—Authentication Success/Failure
INFRA-**0099**	Ensure all privileged access activities are recorded with the log fields specified in Table 25 (privileged account ID, role/privilege level, action performed, target resource, timestamp, outcome).	**SHOULD**	5.3—Privileged Access
INFRA-**0100**	**MUST NOT** use generic Admin accounts for Privileged Access. Assign specific accounts to individual users and grant Admin privileges via role-based access.	**MUST**	5.3—Privileged Access
INFRA-**0101**	Ensure all interactions with sensitive data (PHI, PII, FTI) are recorded with the log fields specified in Table 26 (user ID, data element/record accessed, action type, timestamp, source, outcome).	**MUST**	5.3—Data Access (PHI/PII/FTI)

INFRA-**0102**	Ensure Data Access logging mechanisms support HIPAA Privacy Rule compliance, including the ability to identify and document disclosures of PHI per 45 CFR 164.528 and 45 CFR 164.524.	**MUST**	5.3—Data Access (PHI/PII/FTI)
INFRA-**0103**	Ensure all business transaction events are recorded with the log fields specified in Table 27 (user/system initiating transaction, business process type, before/after values, affected entity, timestamp, outcome, source system).	**MUST**	5.3—Business Transactions
INFRA-**0104**	Record all configuration changes with the log fields specified in Table 28 (user/system, configuration item, before/after values, change type, timestamp, approval reference, outcome).	**MUST**	5.3—Configuration Changes
INFRA-**0105**	Include cross-cutting log fields (Session ID, Transaction ID, Cross-System Linkage, Event Severity, Data Sensitivity Tag) per Table 29 in all log records.	**MUST**	5.3—Cross-Cutting Log Fields
INFRA-**0106**	Ensure access and changes to Medicaid data are logged and traceable.	**MUST**	5.3—Log Characteristics
INFRA-**0107**	Ensure MES components synchronize system clocks to a common authoritative time source for the origin of log events.	**MUST**	5.3—Log Characteristics
INFRA-**0108**	Forward logs to the OHIP SIEM centralized logging solution for aggregation and correlation.	**MUST**	5.3—Log Characteristics
INFRA-**0109**	Protect logs against unauthorized access, modification, or deletion.	**MUST**	5.3—Log Characteristics
INFRA-**0110**	Actively monitor and review logs.	**MUST**	5.3—Log Characteristics
INFRA-**0111**	Retain logs in accordance with federal, New York State, and OHIP regulations and Medicaid Program requirements.	**MUST**	5.3—Log Characteristics
INFRA-**0112**	Ensure logs support filtering, querying, and reporting capabilities.	**MUST**	5.3—Log Characteristics
INFRA-**0113**	Ensure logs support traceability of events back to individual systems.	**MUST**	5.3—Log Characteristics
INFRA-**0114**	Ensure logs support integration by feeding incident response tools and audit reporting systems.	**MUST**	5.3—Log Characteristics
INFRA-**0115**	**MUST NOT** log sensitive data without explicit direction from OHIP. Sensitive data includes PHI, PII, FTI, SSA-supplied data, and MCD.	**MUST**	5.4—Sensitive Data Log Restrictions
INFRA-**0116**	PII deemed sensitive **MUST** only be used in logs with OHIP approval.	**MUST**	5.4—Personally Identifiable Information
INFRA-**0117**	If OHIP directs specific sensitive data to be logged, such logs **MUST** be protected with equal measures as are applied to the protection of the sensitive data itself.	**MUST**	5.4—Sensitive Data Log Restrictions
INFRA-**0118**	Adhere to the log file retention times specified in Table 8 (FTI: 7 years; FTI tracking: 5 years; ePHI: 6 years; PII: 90 days online + 10 years archived; system access: 3 months; production logs: 3 months minimum; non-production: 3 months minimum).	**MUST**	5.5—Retention Periods
INFRA-**0119**	Work with OHIP to move logs to an OHIP-designated location before destruction if logs must be retained beyond their designated retention period.	**MUST**	5.5—Retention Periods
INFRA-**0120**	If a log file contains multiple types of data with different retention periods, the longest retention period **MUST** be used.	**MUST**	5.5—Retention Periods

Section 6.0—Ongoing Licensing and Support Standard | INFRA-0121 to INFRA-0161 | 41 Requirements: MUST 40 | SHOULD 0 | MAY 1			
INFRA-**0121**	All MES solutions and third-party software **MUST** comply with CMS SMC Outcomes and Metrics (including security, risk management, and continuous improvement) and applicable NYS policies.	**MUST**	6.2—Objectives
INFRA-**0122**	Align procured MES components with NYS Medicaid program business, regulatory, and performance expectations.	**MUST**	6.3—Roles and Requirements
INFRA-**0123**	Operate in accordance with CMS regulations for enhanced funding, NYS governance policies, and OHIP MES Standards.	**MUST**	6.3—Roles and Requirements
INFRA-**0124**	Conduct market research to identify and present software options meeting OHIP's needs; handle inquiries, triage incidents, and provide Tier 1/Tier 2 support.	**MUST**	6.3—Roles and Requirements
INFRA-**0125**	Act as primary liaison between OHIP and third-party technology providers, coordinating onboarding, escalations, and issue resolution.	**MUST**	6.3—Roles and Requirements
INFRA-**0126**	Obtain, maintain, and make accessible to OHIP all documentation and agreements pertaining to MES solutions or third-party technology.	**MUST**	6.3—Roles and Requirements
INFRA-**0127**	Develop and submit a comprehensive business case/justification before any MES solution development or third-party procurement that demonstrates business value, links to the APD, documents CMS funding rationale, explains why existing systems are insufficient, and presents risk mitigation.	**MUST**	6.4—Initial Justification
INFRA-**0128**	Submit a comprehensive documentation packet including: product datasheet, draft licensing agreements, documentation of OHIP rights and license transferability, security and privacy compliance documentation, and TCO estimate consistent with CMS APD policies.	**MUST**	6.4—Documentation Requirements
INFRA-**0129**	The Contractor **MAY** be required to submit a Proof of Concept that is collaboratively scoped with OHIP, executed in a non-production environment, evaluated for performance and compliance, and formally documented as part of the approval package.	**MAY**	6.4—Proof of Concept
INFRA-**0130**	Submit all supporting materials (licensing, security, cost, risk assessments, POC results) to OHIP for formal approval gate review before procuring, deploying, or funding any solution under CMS federal matching.	**MUST**	6.4—Formal Approval Gate
INFRA-**0131**	Ensure all approvals are traceable to OHIP APD library and MES solutions inventory. Submit the solution for re-approval if it undergoes significant change in scope, cost, licensing terms, or Contractor relationship.	**MUST**	6.4—Formal Approval Gate
INFRA-**0132**	Submit a comprehensive TCO analysis reflecting the full financial footprint across a 5-to-7-year life cycle, including: license fees, pricing models, implementation costs, integration costs, ongoing maintenance, training, EOL strategy, and Contractor lock-in mitigation.	**MUST**	6.5—Required Elements of TCO Assessment
INFRA-**0133**	Calculate TCO over an OHIP-defined life cycle (5-year for COTS/SaaS, 7-year for foundational platforms), accounting for APDs, certification timelines, technology refresh cycles, documented cost assumptions, and scenario-based modeling.	**SHOULD**	6.5—Life Cycle-Based TCO Calculations

INFRA-**0134**	Ensure all MES and third-party licenses are issued to secure OHIP's legal and operational control, executed in OHIP's name wherever feasible, and include rights of transfer and termination.	**MUST**	6.6—Software Licenses
INFRA-**0135**	Software license contracts **MUST**: articulate OHIP's right to assign licenses to successors, outline penalty-free termination conditions, disclose usage restrictions, and guarantee OHIP's right to reuse licenses without proprietary barriers.	**MUST**	6.6—Software Licenses
INFRA-**0136**	Formally codify OHIP ownership of all operational assets and IP in all contracts, licenses, and service agreements.	**MUST**	6.6—Ownership Rights
INFRA-**0137**	Acknowledge OHIP's exclusive ownership rights; guarantee unrestricted access to raw and processed data; be prohibited from secondary use of OHIP data without written authorization.	**MUST**	6.6—Ownership Rights
INFRA-**0138**	Comply with HIPAA, 42 C.F.R. Part 2, CMS SMC Security Outcomes, and NYS ITS-P19-002 Cloud Computing Policy.	**MUST**	6.6—Ownership Rights
INFRA-**0139**	Provide comprehensive configuration documentation and deliver access to source code, object definitions, or parameter settings for future reuse, where applicable.	**MUST**	6.6—Ownership Rights
INFRA-**0140**	Maintain defined, measurable, and enforceable support and maintenance protocols. Establish a formal SLA with OHIP covering MES solutions and third-party technology.	**MUST**	6.7—Support and Maintenance Governance
INFRA-**0141**	Each SLA **MUST** define system availability, uptime guarantees, tiered response/resolution timeframes, change management protocols, and stakeholder communication pathways. SLA provisions **MUST** align with CMS SMC Outcome #17 and NYS ITS Policies.	**MUST**	6.7—Support and Maintenance Governance
INFRA-**0142**	Define and maintain a detailed incident escalation pathway with tiered support roles (Contractor Tier 1, third-party Tier 2), handoff procedures, and designated contacts for urgent events.	**MUST**	6.7—Support and Maintenance Governance
INFRA-**0143**	Implement periodic reporting to OHIP on maintenance and performance outcomes. Submit reports on OHIP-defined cadence including SLA compliance, ticket volume, incident severity, resolution times, and remediation plans.	**MUST**	6.7—Support and Maintenance Governance
INFRA-**0144**	Submit detailed maintenance plans and schedules to OHIP for approval. Comply with the OHIP Technical Change Control Standard. Document Rollback Plans for recoverability.	**MUST**	6.7—Maintenance Scheduling
INFRA-**0145**	Schedule maintenance to avoid conflicts with critical NYS Medicaid business cycles. Engage in recurring performance meetings with OHIP to review SLA metrics.	**MUST**	6.7—Maintenance Scheduling
INFRA-**0146**	Comply with all applicable security and privacy policies, controls, NYS and federal laws for IT systems that transfer, process, or store OHIP data.	**MUST**	6.8—Security and Compliance Oversight
INFRA-**0147**	Demonstrate compliance by providing documentation and artifacts showing standards and controls are implemented correctly and producing desired outcomes.	**MUST**	6.8—Security and Compliance Oversight
INFRA-**0148**	All software used in the MES environment **MUST** be capable of seamless, standards-based integration with existing NYS Medicaid solutions.	**MUST**	6.9—Integration and Interoperability

INFRA-**0149**	Proposed software **MUST** interoperate with shared NYS infrastructure and comply with CMS, ONC, and OHIP interoperability requirements for clinical, eligibility, or claims data exchange.	**MUST**	6.9—Integration and Interoperability
INFRA-**0150**	Provide comprehensive training and knowledge transfer for OHIP staff, including role-specific curricula, diagnostics instruction, full documentation suite (user manuals, SOPs, configuration docs), in editable version-controlled formats.	**SHOULD**	6.10—Training and Knowledge Transfer
INFRA-**0151**	Complete initial training prior to go-live; validate through ORR process; deliver on schedule with completion checklists signed by OHIP personnel.	**MUST**	6.10—Training and Knowledge Transfer
INFRA-**0152**	Obtain OHIP approval for all training curricula, materials, schedules, and attendee lists prior to rollout. Provide refresher training following major upgrades or configuration changes.	**MUST**	6.10—Training and Knowledge Transfer
INFRA-**0153**	All Contracts **MUST** include tri-party or Contractor-mediated agreements preserving OHIP's access to third-party support, and **MUST** structure disengagement to preserve data integrity and interoperability.	**MUST**	6.11—Contractual Controls and Escalation
INFRA-**0154**	Document, maintain, and integrate multi-tiered escalation protocols within a service management plan, including tiered response levels, designated contacts, timelines, and OHIP intervention points.	**SHOULD**	6.11—Contractual Controls and Escalation
INFRA-**0155**	Provide OHIP with operational and financial reports including: performance and issue logs on OHIP-defined cadence with SLA mapping, root cause analysis, and trend analysis.	**SHOULD**	6.12—Audit and Reporting
INFRA-**0156**	Deliver license and support utilization reports on agreed cadence, detailing license distribution, utilization patterns, access control anomalies, and third-party support interactions.	**SHOULD**	6.12—Audit and Reporting
INFRA-**0157**	Maintain evidence of patch management practices and SLA compliance per the OHIP Security and Privacy Compliance Standard. Comply with FinOps reporting per the Section 7.0 (Cloud FinOps).	**MUST**	6.12—Audit and Reporting
INFRA-**0158**	Maintain detailed and itemized invoice records for a minimum of six (6) years per NYS OSC fiscal retention policies and 2 C.F.R. Part 200.	**MUST**	6.12—OHIP Audits
INFRA-**0159**	Fully cooperate with internal OHIP auditors and any external audit entities authorized by OHIP or CMS.	**MUST**	6.12—OHIP Audits
INFRA-**0160**	Develop and maintain a comprehensive exit and transition strategy for all MES solutions, submitted at initial implementation and updated throughout the contract term.	**SHOULD**	6.13—Exit and Transition Planning
INFRA-**0161**	Upon contract termination or expiration: transfer all configuration artifacts, documentation, and licenses to OHIP; reassign licenses; ensure data export capability in non-proprietary formats (CSV, JSON, XML) with data dictionaries and schema mappings; facilitate HIPAA-compliant secure transfers.	**MUST**	6.13—Exit and Transition Planning
Section 7.0—Cloud FinOps Standard | INFRA-0162 to INFRA-0186 | 25 Requirements: MUST 24 | SHOULD 0 | MAY 1			
INFRA-**0162**	Develop solutions that provide for Cloud FinOps usage, traceability, and reporting requirements.	**MUST**	7.3—Cloud FinOps Oversight

INFRA-**0163**	Collaborate with State-identified resources bearing accountability for OHIP FinOps oversight to establish clear practices for each OHIP solution or portfolio of solutions.	**MUST**	7.3—Cloud FinOps Oversight
INFRA-**0164**	Comply with OHIP's FinOps processes by providing the necessary cost/usage visibility, participating in relevant reviews, and supporting OHIP-led optimization efforts.	**MUST**	7.3—Cloud FinOps Oversight
INFRA-**0165**	Incorporate the collection of cost data consisting of granular cost data from the service provider (with all accompanying tags) and usage data (e.g., number of users, transactions, licensed seats).	**MUST**	7.4—Cost Consolidation
INFRA-**0166**	Update cost and usage data each time the service provider executes a cost update.	**MUST**	7.4—Cost Consolidation
INFRA-**0167**	Securely transmit each solution's ongoing cost data and invoices to OHIP's primary cost reporting solution for enterprise visibility.	**MUST**	7.4—Cost Consolidation
INFRA-**0168**	The Contractor **MAY** utilize a framework such as Focus™ for normalizing cost data; this is encouraged but not required.	**MAY**	7.4—Cost Consolidation
INFRA-**0169**	Provide cost data at the contract and business unit level such that reports on each OHIP-specified environment can be used for show-back/charge-back.	**MUST**	7.4—Cost Allocation
INFRA-**0170**	Produce cost information that facilitates: visibility into spending and accountability, compliance with OHIP charge-back reporting requirements, and Federal Financial Participation (FFP) allocation separating APD and non-APD charges per 42 CFR § 433.112.	**MUST**	7.4—Cost Allocation
INFRA-**0171**	Provide a Monthly Cloud Usage and Spend Report as dashboard content accessible by Business, Finance, and Technical teams, leveraging account structures and usage metrics, detailing spend-trends, budget variance, key cost drivers, and contract context.	**SHOULD**	7.4—Cost Visibility and Reporting
INFRA-**0172**	Work with OHIP to add attribution and costs to regular OHIP cost reports or add new cost reports as required.	**MUST**	7.4—Cost Visibility and Reporting
INFRA-**0173**	Comply with the monitoring requirement established by the Office of the New York State Comptroller (OSC) as part of Procurement and Contract Management.	**MUST**	7.4—Attribution and Usage Monitoring
INFRA-**0174**	Monitor and log resource usage attributable to contracts, program areas, specific staff, services, or functions as required by OHIP, leveraging provider logs and application-level instrumentation.	**MUST**	7.4—Attribution and Usage Monitoring
INFRA-**0175**	Ensure monitoring occurs no less frequently than monthly and is frequent enough to detect, alert, and manage unexpected cost and usage irregularities in a timely manner.	**SHOULD**	7.4—Attribution and Usage Monitoring
INFRA-**0176**	Ensure alerts are triggered when forecast costs exceed agreed limits and that evaluation of costs against forecast for alerting purposes **MUST** be at least daily.	**SHOULD**	7.4—Attribution and Usage Monitoring
INFRA-**0177**	For new solutions, provide OHIP with an estimation of forecasted cloud costs utilizing cloud estimation tools where available, and provide the tool's output along with the estimations.	**SHOULD**	7.4—Initial Cost Estimations
INFRA-**0178**	Base estimated costs on all expected cloud workloads and deployment timeframes.	**MUST**	7.4—Initial Cost Estimations

INFRA-**0179**	Submit a Cloud FinOps plan that aligns spending with business priorities and identifies cost-saving opportunities.	**MUST**	7.4—Budgeting and Financial Tracking
INFRA-**0180**	Define resource usage budgets for all OHIP solutions, including those with significant or variable cloud spend.	**MUST**	7.4—Budgeting and Financial Tracking
INFRA-**0181**	Actively track actual usage spend against usage budgets with established processes for variance assessment, alerting, and review.	**MUST**	7.4—Budgeting and Financial Tracking
INFRA-**0182**	Establish a process for Cloud FinOps collaboration with OHIP to forecast future costs based on historical data, planned architectural changes, anticipated usage patterns, and known cost model changes.	**SHOULD**	7.4—Cost Forecasting and Predictability
INFRA-**0183**	Conduct solution cost optimization reviews on a cadence agreed upon with OHIP, considering right-sizing, optimal pricing models, waste elimination, and architectural efficiency.	**MUST**	7.5—Cost Optimization and Efficiency
INFRA-**0184**	Architecturally isolate OHIP environments (PROD, Dev, SIT, UAT, and distinct functional components) by using separate cloud accounts whenever feasible, resulting in automatically separated costs by environment.	**MUST**	7.5—Architectural Isolation
INFRA-**0185**	Where architectural isolation is not practical, apply and adhere to a minimal, defined, and policy-enforced tagging strategy to all cloud resources.	**MUST**	7.5—Resource Tagging
INFRA-**0186**	Ensure mandatory tags focus on essential identifiers not easily derived otherwise (e.g., Application ID, primary Cost Center).	**MUST**	7.5—Resource Tagging
Section 8.0—Preferred Operational Tools Standard | INFRA-0188 to INFRA-0201 | 14 Requirements: MUST 13 | SHOULD 1 | MAY 0			
INFRA-**0187**	All solutions that do not fit within the definition of OHIP's SaaS model **MUST** comply with this standard.	**MUST**	8.3—Contractor Tool Use
INFRA-**0188**	The Contractor **MUST** refer to and comply with the technologies listed in the OHIP Preferred Operational Tools List for any customized enterprise solution implementation or enhancement.	**MUST**	8.3—Contractor Tool Use
INFRA-**0189**	Ensure team members are familiar with OHIP's published guidance and integrate the usage protocols in their workflow.	**MUST**	8.3—Contractor Tool Use
INFRA-**0190**	Remain aligned with OHIP's updates or modifications to the guidance and adapt processes accordingly.	**MUST**	8.3—Contractor Tool Use
INFRA-**0191**	Obtain OHIP approval for any variation to this standard in the Contract.	**MUST**	8.3—Contractor Tool Use
INFRA-**0192**	Follow Open-Source Project Security Baseline and ISO/IEC 5230 if open-source software is used in solutions.	**SHOULD**	8.3—Contractor Tool Use
INFRA-**0193**	Propose and seek OHIP approval for any additional or alternate technologies other than those listed in OHIP's Preferred Operational Tools List.	**MUST**	8.3—Contractor Tool Use
INFRA-**0194**	For on-premises solutions, seek OHIP's review and approval of technology usage on a case-by-case basis.	**MUST**	8.3—Contractor Tool Use
INFRA-**0195**	All Open-Source Software **MUST** be implemented in accordance with ITS-P019-005.	**MUST**	8.3.1—Open-Source Software
INFRA-**0196**	To be reviewed for approval, OSS **MUST** meet four minimum conditions: free to use, source code available on the Internet, license approved by DOH DLA, and no unapproved terms or conditions.	**MUST**	8.3.1—Open-Source Software

INFRA-**0197**	OSS options **SHOULD** be considered first for all potential software solutions.	**SHOULD**	8.3.1—Open-Source Software
INFRA-**0198**	The Contractor using OSS **MUST** comply with: ISO/IEC 5230 (OpenChain) Standard, OpenSSF ASVS, applicable interoperability standards (W3C, Cloud Native Computing Foundation), and open-source license requirements.	**MUST**	8.3.1—Open-Source Software
INFRA-**0199**	The Contractor **MUST** implement tools and processes to ensure adherence to open-source licenses (strong copyleft, weak copyleft, and permissive).	**MUST**	8.3.1—Open-Source Software
INFRA-**0200**	The Contractor **MUST** develop comprehensive user documentation that outlines how the open-source software is used in the solution.	**MUST**	8.3.1—Open-Source Software

Appendix C: Performance Category Definitions

Table 16 – Performance Category Definitions

Category	Description
User Interface (UI)	UI is simply the point of human-computer interaction. A user interface enables the end user to interact with or control a device's hardware or software. For example, display screens, mice, keyboards, buttons, app icons, and text fields constitute a user interface. In this case, the definition is specific to the responsiveness and efficiency of the system when a user interacts with said system by uploading, downloading, processing, querying, transferring, etc. The complexity of the interaction will dictate the system's response given security measures, errors, processing, etc.
Application Response Time	Application Response time refers to the time it takes to complete a specific task or operation that is not initiated by a user. This includes the duration of all the processing steps involved in executing the given task, such as data retrieval, transportation time, idle time, computation, analysis, and generating the required output or response. For example, system-initiated processes such as enrolling members, processing encounters. The application processing time can vary depending on various factors, including the complexity of the task, the efficiency of the algorithms and data structures used, the processing power of the hardware running the application, the amount of data involved, and any potential bottlenecks or constraints within the system.
Real-Time Interfaces	Real-time interfaces are designed to transfer data on an as-needed basis. When an application needs to either send or request data immediately, a real-time interface is expected to have a request/response synchronous roundtrip. Examples include Point of Sale System interactions and Member Eligibility Verification such as HIPAA X12 270/271.
Data Queries	Data queries refer to the process of requesting and retrieving specific information from a database or dataset. By using query languages or programming languages, users can extract and manipulate relevant data based on certain criteria or conditions. Data queries allow users to filter, sort, aggregate, and transform data to meet their specific needs and objectives. They can be used to answer questions, identify patterns, perform calculations, generate reports, and make informed decisions based on the information extracted from the database. Queries can range from simple to complex, depending on the complexity of the data to be analyzed and the specific requirements of the user. They typically involve specificity looking for the desired columns, filtering conditions, sorting orders, and joining tables, among other parameters Data Queries includes the time application takes to process the data. This includes the time it takes for the system to receive input, perform necessary computations or operations, and generate output or response.
Image Response Time	Image response time refers to the duration it takes for a computer system to process and display an image artifact that are part of the business transaction or digital image stored in response to a user request or interaction. This includes the time it takes for the system to retrieve the image data from storage, process or resize the image if necessary, and transmit the image data to the user's device for rendering.

Category	Description
	The image response time can be affected by various factors, such as the size and complexity of the image, the speed of the storage and network infrastructure, the processing power of the system, and any potential bottlenecks or congestion in the system.

Table 17 – Performance SLA Reporting Elements

Category	SLA Reporting Elements
User Interface	• Provider Name • Contract Number • Application Name • Performance Period • Page Key • Transaction Type • Request Initiation Datetime • Response Datetime • Response Time (in milliseconds [ms])
Application Response Time	• Provider Name • Contract Number • Application Name • Performance Period • Application • Transaction Type • Request Initiation Datetime • Response Datetime • Response Time (ms)
Real-Time Interface	• Provider Name • Contract Number • Application Name • Performance Period • Interface Key • Request Initiation Datetime • Response Datetime • Response Time (ms)

Data Queries	• Provider • Contract • Application • Performance Period • Data Query Type (e.g., Tier I, Tier II, and Tier III) • Query Initiation Datetime • Query Response Datetime • Response Time (ms)
Image Response Time	• Provider • Contract • Application • Performance Period • Transaction Type (Image) • Image Key • Request Initiation Datetime • Response Datetime • Response Time (ms)

Table 18 – Governance Functions and Responsibilities for Service Model by Roles

	SaaS			P/IaaS		
Governance Functions and Definitions	**OHIP**	**Cloud Service Provider**	**The Contractor**	**OHIP**	**Cloud Service Provider**	**The Contractor**
Cost Management Involves monitoring expenses, adhering to budgets, implementing chargeback models, forecasting costs, and identifying optimization opportunities.		X	X	X		X
Security and Privacy Compliance Encompasses protection of the network, digital assets, data encryption, FedRAMP, SOC2 certification of the environment, use of NIST standards		X	X	X	X	X

Data Management Entails OHIP data access, OHIP data storage, OHIP data transmission, and OHIP data sharing	X		X	X		X
Automation and Orchestration Includes creation and configuration of cloud resources using standardized, automated processes.		X	X	X		X
Identity Baseline Involves using any/all identity management solutions across all cloud platforms used at OHIP.	X	X	X	X	X	X
Performance Management Comprises the monitoring of OHIP's application performance.	X		X	X		X

Appendix D: ITIL 4 Framework Reference

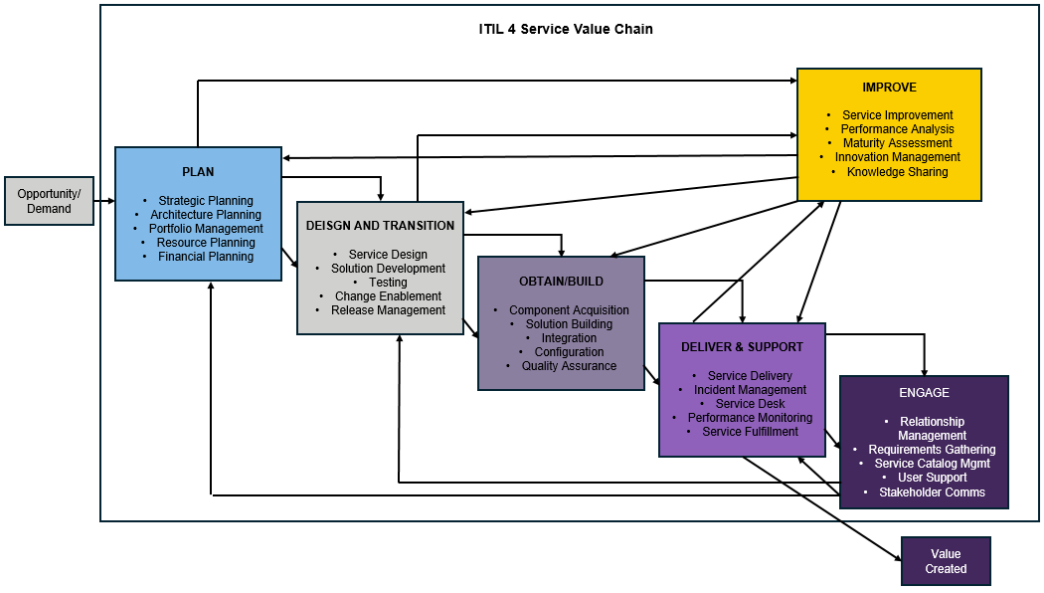
This appendix provides detailed reference information on the ITIL 4 framework that underpins the service management practices defined in this standard. The content is provided for educational and reference purposes to ensure that all stakeholders have access to comprehensive ITIL 4 guidance without requiring separate reference materials.

ITIL 4 is the fourth major version of the IT Infrastructure Library, published by AXELOS. It builds upon decades of IT service management best practices while introducing modern approaches that support digital transformation, Agile methodologies, and DevOps practices. Organizations implementing ITIL 4 benefit from a flexible framework that can be adapted to their specific context while maintaining alignment with globally recognized standards.

Service Value System (SVS) Overview

The ITIL SVS describes how all components and activities of an organization work together to facilitate value creation. The SVS provides a holistic approach to service management and includes the following key components:

- **Guiding Principles**: Seven (7) universal recommendations that guide organizational decisions and actions
- **Governance**: Direction and control mechanisms ensuring the organization acts in accordance with strategy
- **Service Value Chain**: Six (6) interconnected activities that can be combined flexibly to create value streams
- **Practices**: Thirty-four (34) sets of organizational resources designed for performing work or accomplishing objectives
- **Continual Improvement**: Embedded throughout all activities rather than a separate phase



The Seven Guiding Principles

ITIL 4 defines seven (7) guiding principles that **MUST** be considered in every decision and action. These principles are universal and applicable to all organizations regardless of size, context, or methodology. The Contractor **MUST** incorporate these principles into all service management activities.

1. **Focus on Value**: All organization endeavors **MUST** be aligned with creating value for stakeholders. Services **MUST** be designed, delivered, and improved with a clear understanding of stakeholder needs and desired outcomes. The Contractor **MUST** ensure all activities contribute to value realization.

2. **Start Where You Are**: Leverage existing capabilities by assessing the current state, rather than starting from scratch. The Contractor **MUST** evaluate existing processes, technologies, and resources before implementing changes, ensuring improvements are incremental and sustainable.

3. **Progress Iteratively with Feedback**: Adopt a progressive approach by time-boxing iterations with continuous feedback loops. The Contractor **MUST** break large initiatives into manageable pieces, validate progress regularly, and adjust based on feedback to minimize risk and maximize value delivery.

4. **Collaborate and Promote Visibility**: Engage the relevant stakeholders at the right time to ensure the appropriate transparency. The Contractor **MUST** break down silos, engage stakeholders actively, and ensure visibility into work progress and decisions to enable effective collaboration.

5. **Think and Work Holistically**: Recognize that no service stands alone. The Contractor **MUST** consider all four dimensions of service management and the end-to-end integration of services, technologies, and processes to ensure cohesive value delivery.

6. **Keep It Simple and Practical**: Achieve objectives using the minimum number of steps. The Contractor **MUST** eliminate non-value-adding activities, avoid unnecessary complexity, and ensure processes and procedures are practical and usable.

7. **Optimize and Automate**: Maximize the value of work done by human and technical resources. The Contractor **MUST** identify opportunities for automation, optimize resource utilization, and standardize before automating to ensure efficiency gains are sustainable.

The Four Dimensions

ITIL 4 introduces the Four Dimensions Model, which ensures a holistic approach to service management. Every aspect of service management **MUST** consider all four dimensions to ensure effective and efficient value delivery. The Contractor **MUST** address each dimension in their service management approach.

- **Organizations and People**: This dimension addresses organizational culture, structure, roles, competencies, leadership, and workforce planning. The Contractor **MUST** define clear organizational structures and roles that align with OHIP's operating model, ensure appropriate competency frameworks, implement effective change management approaches, and establish communication models that support collaboration.
- **Information and Technology**: This dimension covers information and knowledge management, technologies supporting service management, data architecture, component relationships, automation capabilities, and emerging technologies. The Contractor **MUST** treat information as a

strategic asset, implement knowledge management systems, maintain technology architecture documentation, ensure tool integration, and establish data governance practices.

- **Partners and Suppliers**: This dimension includes relationships with other organizations, contracts, service integration, supplier governance, and ecosystem management. Given OHIP's multi-vendor environment, effective collaboration is essential. The Contractor **MUST** establish vendor management practices, implement contract governance, define integration requirements, support partnership models, and enable value co-creation across the ecosystem.
- **Value Streams and Processes**: This dimension addresses how work is organized and flows, value stream mapping, process design, practice integration, workflow automation, and performance measurement. The Contractor **MUST** define value streams for key services, optimize process efficiency, ensure end-to-end service delivery coordination, implement performance measurement frameworks, and embed continuous improvement.

Service Value Chain

The Service Value Chain is a central element of the SVS. It provides an operating model for service creation, delivery, and continual improvement. Unlike ITIL v3's sequential life cycle, the Service Value Chain consists of six (6) interconnected activities that can be combined in various flexible ways to create value streams tailored to specific scenarios.

1. **Plan**: Ensure a shared understanding of vision, current status, and improvement direction across all four dimensions and products and services. Activities include strategic planning, policy definition, architecture planning, portfolio management, resource planning, and financial planning. The Contractor **MUST** contribute to planning activities as specified in individual contracts.[90]

2. **Improve**: Ensure continual improvement across all value chain activities and throughout the four dimensions. Activities include service and practice improvement, performance analysis, maturity assessment, innovation management, and knowledge sharing. The Contractor **MUST** actively participate in improvement initiatives and maintain improvement registers.

3. **Engage**: Emphasize maintaining strong communication and collaboration with stakeholders to ensure ongoing alignment, transparency, and mutual understanding of service objectives and expectations. Activities include relationship management, requirements gathering, service catalog management, user support, and stakeholder communication. The Contractor **MUST** establish effective engagement mechanisms with OHIP and end users.

4. **Design and Transition**: Ensure products and services meet stakeholder expectations for quality, cost, and time-to-market. Activities include service design, solution development, testing, change enablement, release management, and deployment. The Contractor **MUST** follow OHIP standards for design and transition activities.[91]

---

[90] For more information, refer to the OHIP Program and Project Management Domain Document, Project Management Standard, the OHIP Data and Information Management Domain Document, Data and Naming Standard, and Section 7.0.
[91] For more information, refer to the OHIP Solution Delivery Domain Document, Test Management Standard and Release Management Standard, and the OHIP Program and Project Management Domain Document, Technical Change Control Standard and Project Change Control Standard.

5. **Obtain/Build**: Ensure service components are available when and where needed. Activities include component acquisition, development and integration, infrastructure provisioning, vendor management, and configuration management. The Contractor **MUST** manage the acquisition and building of components in accordance with OHIP procurement and development standards.[92]

6. **Deliver and Support**: Ensure services are delivered and supported according to agreed specifications and stakeholder expectations. Activities include incident management, service request management, service desk operations, monitoring and event management, and problem resolution. The Contractor **MUST** provide ongoing service delivery and support as specified in their contracts.

ITIL 4 Practices Overview

ITIL 4 organizes 34 management practices into three categories. These practices replace ITIL v3's 26 processes with a more holistic approach that recognizes effective service management requires people, information, technology, and suppliers working together, not just process workflows.

- **General Management Practices (14)**: Adapted from general business management domains and applicable across the organization beyond just IT
- **Service Management Practices (17)**: Adapted from traditional ITSM domains and specific to technology service management
- **Technical Management Practices (3)**: Adapted from technology management domains and focused on managing technology components

OHIP has developed requirements for practices that are critical to its operations. Many sections, including the key activities, Contractor's responsibilities, and sample Key Performance Indicators (KPIs), detail these practices. The Contractor **MUST** implement these practices as specified and report on performance regularly.

ITIL Role Descriptions

Process Owner

The Process Owner is the strategic architect of an ITIL process. They possess a holistic view of the organization and how the process contributes to overall business objectives. This role ensures the process aligns with organizational goals and delivers maximum value.

Key Responsibilities:

- **Process Design and Documentation**: Develop the process framework, including policies, workflows, and procedures, and ensure that they are well-documented and accessible to all relevant stakeholders.
- **Alignment with Business Goals**: Ensure the process supports the organization's strategic objectives and contributes to achieving its business goals.
- **Process Improvement**: Lead initiatives for continuous improvement, regularly reviewing and refining the process to enhance efficiency and effectiveness.

---

[92] Refer to the OHIP MES Standards Framework for more information.

- **Stakeholder Engagement**: Engage with key stakeholders to understand their needs and expectations, ensuring that the process delivers value to the business and its customers.
- **Risk Management**: Identify potential risks related to the process and develop mitigation strategies to minimize their impact.
- **Compliance and Governance**: Ensure the process adheres to relevant regulatory requirements and industry standards, maintaining compliance and governance throughout its life cycle.

Process Manager

The Process Manager focuses on the day-to-day management and operational execution of a specific ITIL process. They ensure that the process is implemented correctly and operates within established guidelines.

Key Responsibilities:

- **Operational Oversight**: Supervise the daily activities within the process, ensuring that tasks are completed on time and meet quality standards.
- **Resource Management**: Allocate and manage resources effectively, ensuring that the process is adequately staffed and equipped to meet its objectives.
- **Performance Monitoring**: Track process performance through key performance indicators (KPIs) and metrics, identifying areas for improvement and taking corrective action as needed.
- **Training and Development**: Provide ongoing training and support to process practitioners, ensuring they are well-equipped to carry out their responsibilities.
- **Issue Resolution**: Address and resolve any issues or bottlenecks that arise during the execution of the process, escalating problems when necessary.
- **Reporting**: Prepare regular reports on process performance, risks, and improvement opportunities, sharing insights with the Process Owner and other stakeholders.

Service Owner

The Service Owner is responsible for managing and delivering a specific IT service throughout its life cycle. They ensure that the service meets customer expectations and aligns with organizational objectives.

Key Responsibilities:

- **Service Strategy and Planning**: Develop and implement the service strategy, aligning it with the organization's broader business goals.
- **Service Life Cycle Management**: Oversee the entire service life cycle, from design and deployment to operation and continuous improvement.
- **Customer Relationship Management**: Serve as the primary point of contact for customers and stakeholders, managing relationships and ensuring customer needs are met.
- **Service Level Management**: Monitor and manage service performance against Service Level Agreements (SLAs), ensuring that the service consistently meets or exceeds agreed-upon standards.
- **Financial Management**: Oversee the budgeting and financial performance of the service, ensuring cost-effective delivery without compromising quality.

- **Incident and Problem Management Coordination**: Work closely with Process Owners and Managers to ensure effective incident and problem resolution related to the service.

Process Practitioner

The Process Practitioner is responsible for executing specific tasks within an ITIL process, ensuring that established procedures and standards are followed.

Key Responsibilities:

- **Task Execution**: Perform daily activities related to the process, following guidelines and best practices to ensure consistency and quality.
- **Process Adherence**: Ensure that all tasks are completed in compliance with the defined process, following the steps outlined by the Process Owner and Manager.
- **Documentation and Reporting**: Maintain accurate records of activities and outcomes, documenting any deviations or issues encountered during execution.
- **Collaboration**: Work closely with other practitioners and stakeholders, fostering teamwork and collaboration to achieve process objectives.
- **Feedback and Improvement Suggestions**: Provide feedback to the Process Manager on process performance and suggest potential improvements based on hands-on experience.
- **Incident Handling**: Respond to incidents or issues that arise within the process, escalating them as necessary and contributing to problem-resolution efforts.

NYS ITS and OHIP Role Alignment

To ensure consistent alignment across OHIP vendors and with NYS ITS governance, a standardized role framework has been established that maps ITIL roles to the operational structure defined in the ITS Enterprise Operations Incident Management Process and Policy. This alignment ensures that all parties involved in OHIP service management activities operate with a shared understanding of responsibilities and accountability.

The ITS Incident Management process defines eight core roles that support process execution and management. These roles establish the foundation for how individuals assigned to service management functions will behave and interact within the broader OHIP ecosystem. It is important to note that roles are not equivalent to job titles, and one person **MAY** fill multiple roles while several people **MAY** share a single role depending on operational requirements and organizational structure.

Incident Management Process Owner

The Incident Management Process Owner ensures that the Incident Management process is performed according to agreed and documented procedures while meeting established objectives and requirements. This role is accountable for the proper design, execution, and improvement of the process. The Process Owner ensures that the process is carried out appropriately but does not manage day-to-day operations. Within OHIP, this role is assigned to OHIP Technology Leadership, who maintains ownership of process content and results, documents and enforces process standards, defines team roles and responsibilities, participates in the creation and update of Service Level Objectives, and serves as the representative of the process to all external groups including vendors and state agencies.

Incident Management Process Manager

The Incident Management Process Manager is primarily responsible for the overall quality of the Incident Management process and serves as the main coordinator and focal point regarding process changes.

This role coordinates day-to-day execution, ensures standards and processes are being followed, identifies and addresses exceptions and deviations, and facilitates resolution of issues with items not complying with the process. Within OHIP, this role is assigned to the OHIP System Manager or a designated lead who acts as the focal point for incident management activities, communicates with agencies, Contractors, and management, identifies issues and suggests process improvements, determines tool requirements, and chairs incident review meetings.

Incident Queue Manager

The Incident Queue Manager is responsible for managing assigned ITSM queues for Incident Management to assure that all incident records are acknowledged, assigned, and resolved in accordance with agreed Service Level Objectives (SLO). This role assigns incident records to appropriate resources and monitors timely delivery of service restoration for incidents within assigned groups. Within OHIP, the Incident Queue Manager is designated per system based on the organizational structure of the responsible Contractor. Responsibilities include confirming incident referral correctness and re-routing as needed, ensuring incident records obtain timely assignment, troubleshooting, and resolution, managing incident records near or past their SLO requirements, and explaining queue management results against assigned SLO metrics.

Incident Manager

The Incident Manager provides overall coordination of Major Incidents, monitoring execution activities while managing risks to ensure service and solution delivery commitments are met. This role engages and ensures that all required delivery resources are aligned and available when needed and establishes plans to support continuous improvement efforts. Within OHIP, for cross-vendor incidents, this role is filled by the OHIP Incident Coordinator who determines if an incident **MAY** be categorized as Severity 1, raises severity levels as defined in the process, manages Severity 1 incidents until resolved, executes initial notifications including executive alerts, ensures appropriate teams with appropriate technical and business skills are actively engaged in recovery efforts, coordinates and leads recovery actions for major incidents, and documents accurate timelines of recovery efforts. For vendor-specific incidents, the Vendor Incident Lead at L3 fulfills this responsibility within their domain.

L1 Incident Support Agent

The L1 Incident Support Agent serves as the first line support professional and primary contact for end users. This role is responsible for creating incident records and providing initial support, referring incidents to higher level teams when unable to resolve. Within OHIP, L1 support is provided by the OHIP Contact Center and ITS Enterprise Service Desk. Responsibilities include receiving initial communication of incidents and collecting contact information and incident details, assessing impact and urgency while setting initial severity levels and proper categorization, performing basic troubleshooting using knowledge management resources, attempting resolution via First Contact Resolution, assigning to appropriate Assignment Groups when unable to resolve at L1, following defined severity paths and escalating Severity 1 candidates, rerouting misdirected incidents, confirming incident status and resolution with users, and identifying resolved incidents as candidates for knowledge management.

L2/L3 Incident Support Analyst

The L2/L3 Incident Support Analyst serves as the second line or higher support professional of one or more competency domains. This role provides analysis of incidents and solutions to restore affected services as quickly as possible. Within OHIP, L2 support is provided by OHIP Technical Teams including technical analysts, system administrators, and application support staff. L3 support is provided by the Contractor with deep product expertise. Example responsibilities include confirming incident assignment correctness and re-routing as needed, searching knowledge articles for possible resolutions, updating assigned incidents with work notes in a timely and accurate manner, working cooperatively with other

assignment groups to resolve incidents, creating and executing resolutions via permanent fixes or workarounds, and identifying resolved incidents as candidates for knowledge management.

Incident Communicator

The Incident Communicator is responsible for providing regular business impact notifications to impacted portfolios and agencies during Major Incidents. This role facilitates communication to users and engages stakeholders for decisions regarding restoration, including acceptable risks, timing of outages, and additional changes. Within OHIP, the Incident Communicator works in tandem with the Incident Manager during Severity 1 and Severity 2 events to ensure all affected parties receive timely and accurate information about incident status, expected resolution timeframes, and any workarounds available.

IT Service Owner

The IT Service Owner maintains end-to-end accountability for specific IT service delivery and ensures that services meet customer expectations while aligning with organizational objectives. Within OHIP, Service Owners are designated per system or application and are responsible for service strategy and planning, service life cycle management, customer relationship management, service level management, and coordination of incident and problem management activities related to their assigned services.

OHIP Role Mapping

The following mapping establishes the relationship between ITIL roles, State Enterprise Operations roles, and OHIP operational assignments to ensure consistency across all service management activities.

Table 19 – OHIP Role Mapping

ITIL Role	State Enterprise Operations Role	OHIP Operational Assignment
Process Owner	Incident Management Process Owner	OHIP Technology Leadership
Process Manager	Incident Management Process Manager	OHIP System Manager or designated lead
Queue Manager	Incident Queue Manager	Designated queue owner per system
Incident Manager	Incident Manager	Vendor Incident Lead (L3); OHIP Incident Coordinator (cross-vendor)
L1 Support	L1 Incident Support Agent	OHIP Contact Center; ITS Enterprise Service Desk
L2/L3 Support	L2/L3 Incident Support Analyst	OHIP Technical Teams (L2); Contractors (L3)
Communicator	Incident Communicator	Designated per Major Incident
Service Owner	IT Service Owner	Designated per system or application

Support Tier Model

OHIP operates a multi-tiered support model aligned with industry standards and vendor engagement patterns. The following tier definitions establish consistent terminology across all OHIP systems and Contractors, ensuring clarity in escalation paths and responsibility assignments.

L0 - Self-Service

The L0 tier includes self-service capabilities that enable end-users to resolve issues without human intervention. This tier includes knowledge base access and search functionality, allowing users to find answers to common questions and known issue workarounds. Automated service requests such as password resets and standard access requests are handled at this tier through portal-based systems. Users submit tickets through portal-based forms with guided input that captures necessary information for efficient routing. Where implemented, chatbot and virtual agent assistance provides interactive self-service support.

L1 - Business Support and Contact Center

The L1 tier provides the first point of human contact for end users requiring assistance beyond self-service capabilities. This tier is responsible for initial ticket logging, categorization, and prioritization based on impact and urgency assessment. L1 staff perform basic troubleshooting using knowledge base articles and documented procedures. When issues cannot be resolved at L1, tickets are routed to the appropriate L2 queue based on issue type and system affected. L1 also maintains responsibility for status updates and user communication throughout the ticket life cycle. Responsible parties at this tier include the OHIP Contact Center and OHIP Business Unit Support Teams.

L2 - OHIP Technical Support

The L2 tier provides advanced troubleshooting by OHIP technical staff with deeper technical knowledge of OHIP systems and infrastructure. This tier performs application-level diagnosis and implements configuration changes to resolve issues. L2 staff develop and implement workarounds when permanent fixes are not immediately available. Coordination with L3 vendors occurs when escalation is required due to the need for vendor-specific expertise or code-level access. Technical documentation and knowledge article creation are ongoing responsibilities to improve future resolution efficiency. Responsible parties at this tier include OHIP Technical Analysts, System Administrators, and Application Support Teams.

L3 - Vendor Technical Support

The L3 tier represents vendor-provided technical resources with deep product expertise specific to the solutions they implement and support for OHIP. This tier performs code-level diagnosis and bug identification when issues trace to application defects. Fix development and testing are performed by L3 resources when code changes are required to resolve issues. Performance optimization and tuning activities addressing application-level performance fall within L3 scope. Responsible parties at this tier include Contracted Contractors such as the MECM vendor team, Maximus technical support, and Electronic Medicaid of New York (eMedNY) vendor support. It is important to note that most OHIP vendor contracts specify engagement at this tier rather than at lower support levels.

L4 - Upstream and Sub-contracted Vendor Support

The L4 tier encompasses cloud infrastructure providers, SaaS platform vendors, and third-party component vendors that support underlying technologies used by OHIP systems. This includes cloud infrastructure providers. SaaS platform vendor support for products integrated into OHIP solutions falls within this tier. Third-party component vendors providing specialized functionality or infrastructure services are engaged at L4 when issues trace to their products. Hardware and firmware vendors

supporting physical infrastructure components are also classified at this tier. Responsible parties include vendor support organizations. L4 resources are typically engaged by L3 vendors rather than directly by OHIP. Exceptions to this engagement model require OHIP approval to ensure appropriate coordination and contract compliance.

Appendix E: Citations for OHIP MES Logging Requirements

Federal Standards and Regulations

Table 20 – Security and Privacy Controls for Information Systems and Organizations Audit and Accountability (AU) Control Family

Control	Title	Relevance to MES Logging
AU-2	Audit Events	Requires organizations to determine and log auditable events.
AU-3	Content of Audit Records	Specifies required content elements (user, time, event type, source, outcome).
AU-6	Audit Review, Analysis, and Reporting	Requires review and analysis of audit records.
AU-7	Audit Reduction and Report Generation	Requires capability to query, filter, and report.
AU-8	Time Stamps	Requires synchronized and reliable time stamps.
AU-9	Protection of Audit Information	Requires safeguarding logs from alteration or deletion.
AU-10	Non-Repudiation	Requires ability to associate actions with individuals.
AU-11	Audit Record Retention	Requires retention consistent with policy and regulation.
AU-12	Audit Record Generation	Requires generation of logs for auditable event types.

Related Controls:[93]

- AC-6 – Least Privilege (privileged access logging relevance)
- CM-3 – Configuration Change Control (configuration change logging relevance)

NIST SP 800-92 – Guide to Computer Security Log Management

Relevant Sections:

- Section 2 – Log Generation
- Section 3 – Log Analysis
- Section 4 – Log Storage and Protection
- Appendix A – Recommended Log Elements (source, destination, user, event type, outcome)
- Guidance on correlation identifiers and before/after values for data modifications

Table 21 – HIPAA Security Rule – 45 CFR Part 164 Subpart C

Citation	Requirement
§164.312(b)	Audit Controls – Requires mechanisms to record and examine system activity.

[93] Refer to NIST SP 800-53 Rev. 5.

§164.308(a)(1)(ii)(D)	Information System Activity Review.
§164.308(a)(6)(i)	Security Incident Procedures.
§164.316(b)(2)(i)	Documentation Retention (minimum 6 years).

Table 22 – HIPAA Privacy Rule – 45 CFR Part 164 Subpart E

Citation	Requirement
§164.524	Rights of Access – Supports documentation and traceability of PHI access and release.
§164.528	Accounting of Disclosures – Requires the ability to provide individuals with accounting of certain disclosures of PHI.

Federal Information Security Modernization Act

Requires federal agencies and systems receiving federal funding to:

- Implement NIST-based controls
- Conduct ongoing monitoring
- Maintain audit accountability

CMS Requirements

CMS AMPE Volume I – Acceptable Risk Controls for ACA, Medicaid, and Partner Entities

Relevant AU Controls (aligned to NIST but enhanced operationally):

- AU-02 – Event Logging
- AU-03 – Content of Audit Records
- AU-03(03) – Limit Personally Identifiable Information Elements
- AC-03(01) – Additional Audit Information
- AU-04 – Audit Log Storage Capacity
- AU-05 – Response to Audit Logging Processing Failures
- AU-06 – Audit Record Review, Analysis, and Reporting
- AU-06(01) – Automated Process Integration
- AU-06(03) – Correlate Audit Record Repositories
- AU-07 – Audit Record Reduction and Report Generation
- AU-07(01) – Automatic Processing
- AU-08 – Time Stamps
- AU-09 – Protection of Audit information
- AU-09(04) – Access by Subset of Privileged Users
- AU-10 – Non-Repudiation
- AU-11 – Audit Record Retention
- AU-12 – Audit Record Generation

CMS Acceptable Risk Safeguards (ARS) 5.1

ARS adopts NIST controls and requires:

- Logging of security-relevant events
- Administrative activity monitoring
- Data access traceability
- Centralized log management
- Evidence generation for audits and SMC certification

New York State Requirements

NYS ITS Security Logging Standard (NYS-S14-005)

Relevant Requirements:

- Event logging across applications, databases, OS, network
- Required log content elements
- Centralized log management
- Monitoring and review obligations
- Log retention and disposal requirements
- Restricted log access

NYS ITS Information Security Policy (NYS-P03-002)

Requires:

- Continuous monitoring
- Incident detection
- Compliance validation through logging

Control Element Mapping

Table 23 – Control Element Mapping

Logging Element	Authoritative Source
Authentication Method	NIST SP 800-53 REV. 5 AU-2 + IA-2
Before/After Values	NIST SP 800-53 REV. 5 AU-3; NIST 800-92
Centralized Logging	NIST 800-92; CMS Continuous Monitoring
Configuration Changes	NIST SP 800-53 REV. 5 CM-3; AU-2
Correlation IDs	NIST 800-92
Data Access (PHI/PII)	HIPAA §164.312(b);
Event Type	NIST SP 800-53 REV. 5 AU-3
Log Protection	NIST SP 800-53 REV. 5 AU-9
Log Review Cadence	NIST SP 800-53 REV. 5 AU-6;
Non-Repudiation	NIST SP 800-53 REV. 5 AU-10

Outcome (Success/Failure)	NIST SP 800-53 REV. 5 AU-3;
Privileged Activity	NIST SP 800-53 REV. 5 AU-2; AC-6;
Retention (≥6 years PHI)	HIPAA §164.316(b)(2)(i)
Source (IP/System)	NIST SP 800-53 REV. 5 AU-3; NIST 800-92
Timestamp	NIST SP 800-53 REV. 5 AU-3, AU-8
User ID	NIST SP 800-53 REV. 5 AU-3

Table 24 – Authentication Success/Failure Log Fields

Event Types (Sample)	Log Fields	MES Context (Sample)	Purpose
• Successful login • Failed login attempt • Account lockout • Password reset/change • MFA challenge success/failure • Token issuance /validation (OAuth, Security Assertion Markup Language [SAML], etc.) • Session start/ termination	• User ID (or service account/system ID) • Authentication method (password, MFA, token, certificate) • Timestamp • Source: • IP address • Device ID/ browser/ API client • Target system/ application • Result: • Success • Failure (with reason if available)	• Beneficiary portal login • Provider portal login • Worker eligibility system access • API authentication (e.g., federal data hub, MMIS interfaces) •	• Detect brute-force or credential-stuffing attacks • Establish user session traceability • Support non-repudiation

Table 25 – Privileged Access Log Fields

Event Types (Sample)	Log Fields	MES Context (Sample)	Purpose
• Admin login (separate from standard login) • Role elevation (e.g., temporary privilege escalation)	• Privileged account ID • Role or privilege level (e.g., admin, DBA, system operator) • Action performed	• Eligibility worker role overrides • Provider enrollment admin actions • Claims adjudication overrides	• To address this highest risk activity category • Required for fraud detection and insider

• Creation/ modification/ deletion of user accounts • Changes to roles or permissions • Direct database access by privileged users • Use of “break-glass” emergency accounts (emergency global administrator access)	• Target resource • Timestamp • Source system / IP • Outcome (success/ failure)	• Infrastructure admin actions in cloud or data center	threat monitoring • CMS and NYS expect explicit review of privileged activity

Table 26 – Data Access (PHI/PII/FTI) Log Fields

Event Types (Sample)	Log Fields	MES Context (Sample)	Purpose
• Viewing member eligibility record • Accessing claims history • Exporting data (reports, extracts) • API retrieval of member data • Bulk data access events	• User ID / system ID • Data subject (e.g., member ID) • Data type accessed (PHI, PII, FTI, financial) • Action: • View • Create • Update • Delete • Export / download • Timestamp • Source (IP/system) • Purpose of access (if available)	• Caseworker viewing beneficiary file • Provider accessing patient claim details • Data warehouse query involving PHI • Third-party integration pulling Medicaid data	• Core HIPAA audit requirement • Enables: • Data breach detection • Improper access identification • Data use agreement enforcement

	• Outcome (success/ failure)		

Table 27 – Transactions Log Fields

Event Types (Sample)	Log Fields	MES Context (Sample)	Purpose
• Claims submission, adjudication, payment • Eligibility determination or redetermination • Enrollment/ disenrollment • Provider onboarding or updates • Prior authorization decisions	• Transaction ID • User/system initiating transaction • Business process type • Before/after values (where applicable) • Affected entity (member, provider, claim) • Timestamp • Outcome (success/failure) • Source system/interface	• MMIS claims lifecycle events • Eligibility system updates (MAGI/non-MAGI) • Federal hub verification responses • Managed care enrollment changes	• To ensure program integrity and auditability • Supports: • Fraud, waste, and abuse detection • Financial accountability • CMS reporting and certification

Table 28 – Configuration Changes Log Fields

Event Types (Sample)	Log Fields	MES Context (Sample)	Purpose
• Security configuration changes • Firewall rule updates • IAM policy changes • Application configuration changes • Database schema changes • Deployment of new code releases	• User/system making the change • Configuration item changed • Before/after values • Change type (create/ update/ delete) • Timestamp • Approval reference (if tied to change management) • Outcome (success/failure)	• Changes to eligibility rules engine • Claims pricing configuration updates • Provider reimbursement rules • API endpoint configuration changes	• Detect unauthorized or high-risk changes • Supports: • Change management governance • Root cause analysis • System integrity validation

Table 29 – Cross-Cutting Log Fields

Log Fields	Purpose
• Session ID • Transaction ID • Cross-System Linkage	To support **Correlation**
• Event severity (info, warning, critical) • Data Sensitivity Tag (PHI, PII, FTI, financial)	To support **Classification**

Appendix F: ITSM Suggested KPIs

Table 30 – Continual Improvement Business Suggested KPIs

Continual Improvement Business Suggested KPIs
Number of emergency, expedited, standard and normal changes
Number of changes with different planned vs actual date / time
Unique and recurring number of data fixes
Total number of rows updated by data fixes during batch cycles
Average time on page as defined by OHIP business
Number of printable output errors categorized by type

Table 31 – Continual Improvement System Suggested KPIs

Continual Improvement System Suggested KPIs
Total time of unplanned outages categorized by SEV-1 and SEV-2
Number and total time of planned outages categorized by reason (patching, deployment, etc.)
Average time for simple and complex processes categorized by solution components
Average memory and CPU Utilization categorized by solution or components
Percentage of high response time (based on agreed up thresholds)
Number of SEV-1 and SEV-2 Incidents per reporting period
Number of aging Incidents by severity level
Number of failed batch jobs per reporting period
Number of aging problems by severity level

Table 32 – Continual Improvement Release Suggested KPIs

Continual Improvement Release Suggested KPIs
Number of Change Requests implemented by the Release
Number of defects resolved by the Release
Number of defects by aging groups, severity, rolled up by functional area
Percentage of first run script failures by release for SIT and UAT
Percentage of valid and invalid defects by release for SIT and UAT

Table 33 – Information Security Management Suggested KPIs

Information Security Management Suggested KPIs
Number of systems with known critical and high vulnerabilities
Number of events per service or application

Information Security Management Suggested KPIs
Number of incidents detected
Mean-Time-To-Detect (MTTD)
Mean-Time-To-Resolve (MTTR)
Mean-Time-To-Contain (MTTC)
Number of devices and applications being monitored
Number of unmanaged devices on IS Solution
Average IS Contractor security rating
Mean time for IS the Contractor to respond to security incidents
Number of Plan of Actions & Milestones (POA&M)
Percentage of POA&M's completed in last quarter

Table 34 – Knowledge Management Suggested KPIs

Knowledge Management Suggested KPIs
Average age of knowledge assets created
Percentage of knowledge assets periodically reviewed
Frequency of use of knowledge assets created (e.g., statistical use of organizational/intranet and other knowledge repositories and collaboration platforms)
Consumer satisfaction/feedback with Knowledge Management policies, procedures, tools, and content

Table 35 – Availability Management Suggested KPIs

Availability Management Suggested KPIs
Percentage of unavailability of services and components
Percentage of improvement in overall end-to-end availability of service
Percentage reduction in the number of service breaks
Reliability – mean time between failures (MTBF)
Reliability – mean time between service incidents (MTBSI)
Maintainability – mean time to restore service
Number of critical time failures (e.g., specific business peak and priority availability needs are planned for)

Table 36 – Capacity and Performance Management Suggested KPIs

Capacity and Performance Management Suggested KPIs
Percentage of accuracy of forecast business trends
Variances between actual and forecast capacity
Percentage of urgent procurement requests to address capacity performance issues

Capacity and Performance Management Suggested KPIs
Percentage of IT components over-capacity
Percentage of incidents due to poor capacity performance
Percentage of services and components under capacity monitoring
Percentage of capacity reserves at times of normal and peak demand
Number of Configuration Items under-utilized divided by total number of Configuration Items supported
Number of capacity-related incidents identified and resolved prior to any production impact
Percentage increase in consumer perception and satisfaction of SLA achievements, via service reviews and consumer satisfaction survey responses
Percentage reduction in SLA breaches caused because of vendor partner support contracts
Percentage increase in SLAs met against capacity and availability services being run
Percentage reduction in the costs associated with service provision
Percentage of system performance reviews completed on time

Table 37 – Change Enablement Suggested KPIs

Change Enablement Suggested KPIs
Number of Change Requests submitted
Number of changes that meet consumer expectations
Number of changes implemented within agreed change window
Number of incidents attributed to changes
Number of changes implemented successfully
Number of changes approved for implementation
Number of changes by type (Standard, Normal, Emergency)
Number of open Change Requests
Changes by impact and risk
Number of changes backed out
Total amount of time from when an emergency change is implemented until the record is closed
Total amount of time from when a normal change is submitted until the record is closed
Number of unauthorized changes

Table 38 – Incident Management Suggested KPIs

Incident Management Suggested KPIs
Total number of incidents by priority and by category
Total time to resolve incidents by priority and by category
Number of incidents at each stage (by status)

Incident Management Suggested KPIs
Size of current incident workload for each IT service
Number and percentage of major incidents
Number and percentage of tickets aging longer than defined time periods (e.g., 10 days or 20 days, etc.)
Total number of incidents

Table 39 – Problem Management Suggested KPIs

Problem Management Suggested KPIs
Total number of problems by priority and by category
Total time to resolve problems by priority and by category
Size of current problem workload for each IT service
Number and percentage of major problems resolved
Number and percentage of problem tickets aging longer than defined time periods

Table 40 – Release Management Suggested KPIs

Release Management Suggested KPIs
Number of emergency Releases and out-of-schedule Releases
Number of successful Releases
Number of backed out Releases
Number of changes performed within allocated change windows; number exceeded change windows
Quantity of incidents related to a Release
Number of incidents against the Release of the service
Percentage of blacked-out Releases
Percentage of Releases successfully meeting validation criteria to proceed to planning stage of the Release
Percentage decrease of known errors and defects during testing of the Release
Percentage increase in successful test completions of the Releases
Percentage reduction in Number of incidents due to incorrect components being deployed

Table 41 – Service Configuration Management Suggested KPIs

Service Configuration Management Suggested KPIs
Percentage of accuracy of Configuration Item information
Percentage of reduction in business impact of outages and incidents caused by poor asset and configuration management
Frequency of Configuration Item collection

Service Configuration Management Suggested KPIs
Total number of Configuration Items
Percentage of rolled back changes
Number and severity of breaches in SLAs caused by inaccurate CMDB information
Timeliness of management reports
Percentage of accurate Configuration Items reported during verification and audit
Frequency of unregistered Configuration Items

Table 42 – Service Desk Management Suggested KPIs

Service Desk Management Suggested KPIs
First contact resolution rate by tier
Average handle time
Customer satisfaction scores
Escalation rates
Ticket aging metrics
Percentage of calls handled by L0 without escalation

Table 43 – Service Request Management Suggested KPIs

Service Request Management Suggested KPIs
Percentage of requests fulfilled within SLA
Percentage of unfulfilled requests (e.g., orphaned requests)
Percentage of requests fulfilled that are authorized
Breakdown of requests at each stage including Approval stage
Meantime to fulfil by different parameters such as category, fulfilment group etc.
Average user/consumer survey score (e.g., total and by question category)
Percentage of incidents opened against fulfilled requests
Percentage of requests handled by Tier 1 and fulfilled on first interaction
Total Number of requests (as a control measure)

Table 44 – Service Validation and Testing Suggested KPIs

Service Validation and Testing Suggested KPIs
Increased percentage of evaluations delivered by agreed times
Increased percentage of evaluations not delivered by agreed times
Reduced number of changes that **MUST** be backed out due to unexpected errors or failures
Reduced number of failed changes

Appendix G: Standard Terminology

For the purposes of this standard, the following terms are defined:

- **Contractor**: An external organization that has entered into a formal contract with OHIP to provide IT services, solutions, or support. Contractors include entities such as system integrators, managed service providers, and technology vendors engaged under procurement contracts.
- **Stakeholder**: Any person, group, or organization that can affect, be affected by, or perceive itself to be affected by an aspect of OHIP's IT services. Stakeholders include but are not limited to: OHIP leadership and staff, Contractors, end users (Medicaid recipients, healthcare providers), business managers, technical architects, NYS ITS, federal partners (CMS), and other state agencies that interact with OHIP systems.
- **Supplier**: An organization (internal or external) that provides goods or services used in the delivery of IT services but **MAY** not directly deliver services to OHIP end users. This includes infrastructure component suppliers, software vendors, cloud platform providers, and other third parties in the service delivery chain.[94]
- **Vendor**: An external commercial organization that provides technology products, software licenses, or services to OHIP. Vendors **MAY** provide commercial off-the-shelf (COTS) products, cloud services, or specialized IT solutions. Vendors are a subset of Contractors when they are directly responsible for service delivery to OHIP.
- **Software as a Service (SaaS):** SaaS is a ready-to-use software application accessible by users through a web browser or a dedicated interface over the Internet/Intranet that can be configured/customized for OHIP needs by authorized staff. The SaaS Contractor hosts and manages the application, including infrastructure, middleware, and application software. SaaS offerings could be multi-tenancy with dedicated and secure tenancies for OHIP's use or dedicated implementations for OHIP. SaaS offerings may or may not be subscription-based.
- **Platform as a Service (PaaS):** PaaS is a complete cloud environment that provides all the necessary tools and resources for the Contractor and developers and to build, run, and manage applications. It typically includes cloud infrastructure, middleware software, database management solutions, and a UI. Developers can focus on coding and application logic, while the PaaS provider handles the underlying infrastructure and operating system. The Contractor **MUST** recommend specific types of PaaS based on solution requirements for OHIP evaluation and approval.
- **Infrastructure as a Service (IaaS):** The IaaS model is an infrastructure service that provides on-demand access to computing resources such as servers, storage, virtual machines (VMs), and networking. The Contractor deploys and manages their operating systems, applications, and data within the provided virtualized environment.
- **Protected Health Information (PHI):** As noted by the National Institute of Standards and Technology, PHI is considered individually identifiable health information that is “(i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. Excludes individually identifiable health information in (i) Education records

[94] For more information, refer to the ITIL 4 Supplier Management Practice.

covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer."[95]

- **Individually Identifiable Health Information:** As provided here by the National Institute of Standards and Technology (NIST), individually identifiable health information "is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) identifies the individual; or (ii) concerning which there is a reasonable basis to believe the information can be used to identify the individual."[96]
- **Personally Identifiable Information (PII):** Personally Identifiable Information (PII) is information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), date and place of birth, mother's maiden name, biometric records, including any other personal information which can be linked to an individual PII deemed sensitive must only be used in logs with OHIP approval. NIST SP 800-122 provides guidance on determining filed data sensitivity.[97]
- **Federal Tax Information (FTI):** FTI includes federal tax returns or return information received directly from the IRS or obtained through an authorized secondary source such as SSA. In addition, copies of tax returns or return information provided to the agency directly by the taxpayer or their representatives (e.g., W-2s, Form 1040, etc.) or obtained from public information files are not protected FTI that is subject to the safeguarding requirements of IRC 6103(p)(4).[98]
- **Social Security Administration (SSA) Supplied Data:** SSA supplied data includes records, information, or data received from specific SSA feeds, potentially including names, SSNs, addresses, amounts, and other information related to SSA benefits and earnings information for individuals. This data is subject to Computer Matching and Privacy Protection agreements between OHIP and SSA, which set forth the terms and conditions for the use, disclosure, and disposition of such data.[99] Additional information and requirements on Computer matching can be found in NYS ITS-P22-001.[100]

> ***Note:*** *SSA-provided data can be included in FTI and PII data.*

- **Medicaid Confidential Data (MCD):** The federal Medicaid Confidential Data Standard is established by §1902(a)(7) of the Social Security Act (42 USC §1396a(a)(7)). The law requires that a "State plan for medical assistance must: (7) provide safeguards which restrict the use or

---

[95] To review the source information used for PHI, refer to NIST De-Identification of Personal Information.
[96] For more information, refer to the HIPAA Security Rule NIST SP 800-66 Rev. 2.
[97] For more information, refer to NIST Guide to Protecting the Confidentiality of Personally Identifiable Information.
[98] For more information, refer to IRS Tax Information Security Guidelines.
[99] For more information, refer to Computer Matching Agreement between CMS and State-Based Administering Entities.
[100] For more information, refer to NYS ITS P22-001.

disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the plan." This statutory requirement is implemented in regulations at 42 CFR §431.300 et seq. 42 CFR §431.302 and defines that the Continuing Medicaid Eligibility Modernization Program administration includes:

- Establishing eligibility.
- Determining the amount of medical assistance.
- Providing services for recipients.

Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan.[101]

[101] For more information, refer to Medicaid Confidentiality Regulations and Standards.

Appendix H: Acronyms

The following acronyms are used throughout the OHIP Infrastructure and Operations Domain Document.

ACA: Affordable Care Act
ADA: Americans with Disabilities Act
AMQP: Advanced Message Queuing Protocol
APD: Advance Planning Document
API: Application Programming Interface
ARS: Acceptable Risk Safeguards (CMS)
AS2: Applicability Statement 2
ASC: Accredited Standards Committee
ASVS: Application Security Verification Standard
AWS: Amazon Web Services
BC/DR: Business Continuity and Disaster Recovery
BIA: Business Impact Analysis
BSS: Business Support Services
CAP: Corrective Action Plan
CDD: Cloud Design Document
CEF: Conditions for Enhanced Funding
CFR: Code of Federal Regulations
CI/CD: Continuous Integration / Continuous Deployment
CM: Configuration Management
CMDB: Configuration Management Database
CMS: Centers for Medicare & Medicaid Services
COTS: Commercial Off-The-Shelf
CRER: Contract Reporter Exemption Request
CSI: Continual Service Improvement
CTO: Chief Technology Office
DBA: Database Administrator
DDI: Design, Development, and Implementation
DOH: Department of Health (New York State)
DOS: Division of Operations and Systems (New York State)
DR: Disaster Recovery
E&E: Eligibility and Enrollment
EDA: Event-Driven Architecture
EDI: Electronic Data Interchange
EDW: Enterprise Data Warehouse
eMedNY: Electronic Medicaid of New York
EOL: End of Life
EULA: End-User Licensing Agreement
FFP: Federal Financial Participation
FHIR: Fast Healthcare Interoperability Resources
FIM: File Integrity Monitoring
FTI: Federal Tax Information
GCP: Google Cloud Platform
GRS: General Records Schedule
HIPAA: Health Insurance Portability and Accountability Act
HL7: Health Level Seven
HTTPS: Hypertext Transfer Protocol Secure
IaaS: Infrastructure as a Service
IAM: Identity and Access Management
ICD: Interface Control Document

IP: Internet Protocol
IT: Information Technology
ITAM: IT Asset Management
ITDD: Integration Technical Design Document
ITIL: Information Technology Infrastructure Library
ITS: Office of Information Technology Services (New York State)
ITSM: Information Technology Service Management
JMS: Java Message Service
JSON: JavaScript Object Notation
KPI: Key Performance Indicator
LD: Liquidated Damages
MAGI: Modified Adjusted Gross Income
MCD: Medicaid Confidential Data
MECM: Medicaid Eligibility and Client Management
MES: Medicaid Enterprise System
MFA: Multi-Factor Authentication
MFT: Managed File Transfer
MITA: Medicaid Information Technology Architecture
MMIS: Medicaid Management Information System
M&O: Maintenance and Operations
MQTT: Message Queuing Telemetry Transport
MTBF: Mean Time Between Failures
MTBSI: Mean Time Between Service Incidents
MTTC: Mean Time to Contain
MTTD: Mean Time to Detect
MTTR: Mean Time to Resolve
NARA: National Archives and Records Administration
NIST: National Institute of Standards and Technology
NYS: New York State
OCM: Organizational Change Management
OGS: Office of General Services (New York State)
OHIP: Office of Health Insurance Programs (New York State)
OMB: Office of Management and Budget (New York State)
ONC: Office of the National Coordinator for Health Information Technology (New York State)
ORR: Operational Readiness Review
OS: Operating System
OSC: Office of the State Comptroller
OSS: Open-Source Software
OWASP: Open Web Application Security Project
PaaS: Platform as a Service
PHI: Protected Health Information
PII: Personally Identifiable Information
PM: Project Management
POA&M: Plan of Action and Milestones
QA: Quality Assurance
RTO: Recovery Time Objective
SA: Systems Administration
SaaS: Software as a Service
SADD: System Architecture Design Document
SAML: Security Assertion Markup Language
SBX: Sandbox
SDLC: Solution Development Life Cycle
SDR: Standards Deviation Request
SFTP: Secure File Transfer Protocol
SIEM: Security Information and Event Management
SIT: System Integration Testing

SLA: Service Level Agreement
SLO: Service Level Objective
SMC: Streamlined Modular Certification
SME: Subject Matter Expert
SMTP: Simple Mail Transfer Protocol
SOA: Service-Oriented Architecture
SOC: Security Operations Center
SOP: Standard Operating Procedure
SP: Special Publication (NIST)
SSA: Social Security Administration
SSN: Social Security Number
SSPP: System Security and Privacy Plan
SVS: Service Value System
TAS: Technical Advisory Services
TCO: Total Cost of Ownership
UAT: User Acceptance Testing
UI: User Interface
URI: Uniform Resource Identifier
USC: United States Code
W3C: World Wide Web Consortium
X12: ASC X12 Electronic Data Interchange Standard
XML: Extensible Markup Language