



Security, Privacy, and Compliance Domain Document

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

October 23, 2026

Contents

1.0	Introduction	4
1.1	Purpose.....	4
1.2	Objectives	4
1.3	Authority	5
1.4	Scope	5
1.5	How This Document Is Organized.....	5
1.6	Companion Domain Standards	6
1.7	Compliance Tier Framework	7
1.8	Compliance and Enforcement.....	8
2.0	OHIP Security and Privacy Control Baseline.....	11
2.1	Additional Data Classifications	11
2.2	System Security and Privacy Plan (SSPP).....	12
2.3	Additional System Security Privacy Plan Requirements	12
2.4	Solution Development Life Cycle (SDLC) Change Control	13
2.5	Training and Awareness	13
3.0	Privacy Requirements	13
3.1	Data Use Agreement.....	13
3.2	Data Use Agreement Addendum.....	14
3.3	Names List	14
3.4	Business Associate Agreement (BAA)	14
3.5	Sensitive Data Types.....	15
3.6	Use of Production Data Restrictions	15
3.7	De-Identification Restrictions.....	15
4.0	Zero Trust.....	16
4.1	Encryption	17
4.2	Identity and Access Management (IAM).....	18
4.3	Interface Authorization	18
4.4	Proper Use of Service Accounts.....	19

4.5	Secure API Development	19
4.6	AI Security and Privacy	20
4.7	Database Security Requirements.....	20
5.0	Enterprise Security Architecture	21
5.1	Comingling Restrictions.....	21
6.0	Cloud Security.....	22
6.1	Federal Risk and Authorization Management Program (FedRAMP) Authorization	22
6.2	Contractor Cloud Compliance	22
6.3	Automated Compliance Cloud Tools	23
6.4	Onshore Compliance	23
6.5	Software-as-a-Service (SaaS).....	23
7.0	Logging and Continuous Monitoring.....	24
7.1	Continuous Security Operations.....	24
7.2	Security Information and Event Management (SIEM)	24
8.0	Certification and Operational Compliance	24
8.1	Framework and Processes.....	24
8.2	Certification Support.....	24
8.3	Asset Management and System Inventory.....	25
8.4	System/Solution Audit Support and Management.....	25
8.5	Vulnerability Scanning and Reporting	25
8.6	Application Security Testing and Reporting	26
8.7	Penetration Testing and Reporting	26
8.8	Incident Management and Reporting	26
9.0	Contact Information	26
10.0	Revision History	26
	Appendices	28
	Appendix A: Deliverables and Artifacts.....	29
	Appendix B: Master Requirements Summary	35
	Appendix C: Legal and Regulatory Compliance.....	42
	Appendix D: Acronyms.....	43

Table of Tables

Table 1 – How this Document is Organized	6
Table 2 – Companion Domain Standards	6
Table 3 – Compliance Tier Framework	7
Table 4 – Domain Requirements Summary	8
Table 5 – Deliverables and Artifacts.....	29
Table 6 – Master Requirements Summary Table	35

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

1.0 Introduction

1.1 Purpose

The Security and Privacy Compliance Standard establishes security and privacy requirements based on the Office of Health Insurance Programs (OHIP) Security and Privacy Controls Baseline and associated procedures for protecting OHIP data, including but not limited to:

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Personal, Private or Sensitive Information (PPSI)
- Medicaid Confidential Data (MCD)
- Federal Tax Information (FTI)
- Affordable Care Act (ACA) Information
- Social Security Administration (SSA) Information
- Medicare data

This Standard ensures compliance with both federal (i.e., Centers for Medicare and Medicaid Services [CMS] Acceptable Risk Safeguards [ARS] and National Institute of Standards and Technology [NIST] SP 800-53) and New York State (NYS) requirements while mitigating information security and privacy risks related to creating, transferring, processing, maintaining, transmitting, or storing OHIP data. For the purpose of this Standard, OHIP data is any data created, transferred, processed, maintained, transmitted, or stored by OHIP to conduct Medicaid program business, regardless of whether or not that data originated with OHIP. Deliverables and artifacts associated with this standard can be found in [Appendix A](#).

1.2 Objectives

The objectives of this Standard are to:

- Ensure adherence to the OHIP Security and Privacy Controls Baseline for any system that will create, transfer, process, maintain, transmit, or store OHIP data, as noted in [Section 1.1](#) of this Standard.
- Inform prospective vendors of the requirements related to developing a standardized System Security and Privacy Plan (SSPP) in support of any OHIP contracted work. The SSPP will be used by the OHIP Security and Privacy Team to assess and monitor progress towards compliance with this standard.

- Identify the requirement to execute Data Use Agreements (DUAs) and Business Associate Agreements (BAAs) to govern the legal use, sharing, and protection of OHIP data as provided in [Section 1.1](#) of this Standard.
- Establish a repository for reference documentation to support OHIP's requirements for compliance with baseline security and privacy standards. The repository **MUST** be accessible by internal and external OHIP stakeholders as well as potential vendors engaged in OHIP Information Systems projects.

1.3 Authority

The New York State 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 New York State 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 Medicaid Enterprise System (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 PHI, PII, MCD, IRS 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	Security and Privacy Control Baseline
Section 3.0	Privacy Requirements
Section 4.0	Zero Trust, Encryption, IAM and Database Security
Section 5.0	Enterprise Security Architecture
Section 6.0	Cloud Security
Section 7.0	Logging and Continuous Monitoring
Section 8.0	Certification and Operational Compliance

1.6 Companion Domain 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 Domain Standards

OHIP Standard	Domain	Scope Relationship
OHIP Artificial Intelligence (AI) Security and Privacy Standards Baseline	External OHIP Security	Establishes baseline security and privacy standards for AI systems and services used by OHIP (the NYS Office of Health Insurance Programs). It explains why AI poses unique risks beyond traditional software, including adversarial attacks on models, LLM-specific data exposure, and the emerging threat surface of agentic AI and sets out guiding principles and attribute standards for procuring, developing, and risk-assessing any AI system that touches Sensitive/Confidential data (Medicaid Confidential Data, PHI/PII, mental health, reproductive health, etc.).
OHIP Secure Application Programming Interface (API) Development Standards Baseline	External OHIP Security	Defines baseline security standards for developing and operating APIs (both internal and external, including microservices) that access or transmit Sensitive/Confidential data tied to the NYS Medicaid program. Aligned with NIST SP 800-228 and standards from the Internet Engineering Task Order (IETF), Open Web Application Security Project (OWASP), and the OpenID Foundation, it emphasizes that the same controls apply regardless of whether a caller is internal or external, with particular focus on OAuth 2.0/Representational State Transfer (REST) security in the context of CMS and ONC regulatory mandates (like the Patient Access API under CMS-9115-F and CMS-0057-F). Like its AI counterpart, it's a high-level summary that defers to a detailed Technical Guidance document for implementation specifics.

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 Standards Deviation Request (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 SMC certification 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

An 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 **MUST** 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
Security and Privacy Control Baseline	2.0	SEC-0001 – SEC-0013	11	2	0	13
Privacy Requirements	3.0	SEC-0014 – SEC-0030	17	0	0	17
Zero Trust, Encryption, IAM and Database Security	4.0	SEC-0031 – SEC-0062	26	6	0	32
Enterprise Security Architecture	5.0	SEC-0063 – SEC-0069	4	3	0	7
Cloud Security	6.0	SEC-0070 – SEC-0080	9	2	0	11
Logging and Continuous Monitoring	7.0	SEC-0081 – SEC-0082	2	0	0	2
Certification and Operational Compliance	8.0	SEC-0083 – SEC-0098	13	3	0	16
Total			82	16	0	98

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, data, 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 OHIP Security and Privacy Control Baseline

Any system that stores, processes, accesses, or transmits OHIP data **MUST** comply with the Department of Health OHIP Security and Privacy Controls Baseline. This Baseline:

- Governs the data classification associated with the data that is stored, processed, analyzed, or transmitted by the system (solution).
- Covers all OHIP data classifications, including but not limited to, those defined in [Section 1.1](#) of this Standard, at OHIP's sole discretion.

All MES solutions **MUST** follow the latest versions of the following governances: Either CMS ARS¹ or CMS ARC-AMPE when solution is required to connect directly to the Fed Hub, NYS Cybersecurity Policies and Standards,² and any federal or State laws applicable to the data contained within. It **SHOULD** also be understood that:

- OHIP created specific security and privacy control family workbook templates that will be provided to the Contractor upon contract award.
- All federal agency security and privacy control baselines follow the latest version of the NIST 800-53 standards at the NIST / CMS Moderate impact level.
- OHIP added additional controls to their Security and Privacy Control Baseline to better align with NYS Cybersecurity policies and standards. As such, this Baseline falls between the Moderate and High impact level.

Further, OHIP has leveraged national security and privacy standards and best practices to develop application-specific standards related to the use of Artificial Intelligence (AI) technologies and Application Programming Interface (API). These standards **MUST** be followed where deemed applicable at the sole discretion of OHIP. In addition to this, the OHIP Security and Privacy Compliance Standard, OHIP Secure API Development Baseline, and OHIP Secure AI Security and Privacy Baseline will be provided as part of the procurement library.

2.1 Additional Data Classifications

In addition to PII, PHI, PPSI, and MCD, additional security and privacy control requirements may apply when other data types are stored, processed, accessed, and/or transferred via the system. Examples include, but are not limited to:

- **FTI Data:** If applicable, the IRS Publication 1075 Security and Privacy Control Baseline **MUST** be followed. OHIP has developed an IRS Overlay Control workbook to include additional controls. These controls are necessary to fulfill the IRS Publication 1075 required controls not already included in the OHIP Security and Privacy Controls Baseline.
- **ACA Data:** If applicable, the CMS ARC-AMPE Security and Privacy Control Baseline **MUST** be followed. OHIP has developed an ACA Overlay Control workbook to include additional controls.

¹ For more information, refer to the [CMS Acceptable Risk Safeguards \(ARS\) | CMS Information Security and Privacy Program](#).

² For more information, refer to ITS Cybersecurity Policies and Standards at [Policies | Office of Information Technology Services](#).

These controls are necessary to fulfill the IRS Technical System Security Requirements (TSSR) required controls not already included in the OHIP Security and Privacy Controls Baseline.

- **SSA Data:** If applicable, the SSA TSSR Security and Privacy Control Baseline **MUST** be followed. OHIP has developed an SSA Overlay Control workbook to include additional controls which are required to comply with IRS TSSR required controls that are not already included in the OHIP Security and Privacy Controls Baseline.
- **Medicare Data:** Medicare data are obtained from CMS for care coordination, quality improvement, and third-party liability activities. All security and privacy requirements are derived from CMS requirements.

2.2 System Security and Privacy Plan (SSPP)

Contractors **MUST** demonstrate compliance with the SSPP. This may be accomplished through a variety of methods, such as through the completion of SSPP workbooks, HITRUST certification with New York State compliance overlay, attestation with third-party audit, and others, at the sole discretion of the Department.

The Contractor **MUST** complete the SSPP workbooks and any additional applicable data classification workbook overlays. When completing these workbooks, the Contractor **MUST** explain in detail how each control and control requirement has been implemented. The Contractor **MUST** also provide supporting artifacts as evidence of implementation.

- OHIP reserves the right to independently test and verify security and privacy controls as deemed necessary. The expectation is that OHIP has access to Acceptance Testing infrastructure and Production infrastructure for such testing. This includes testing and verifying appropriate security and privacy controls for any changes to architecture or security systems before they are implemented in the production environment. Contractors **MUST** include allowances for OHIP to independently test any security and privacy controls in their workplans. This testing includes, but is not limited to, penetration testing and vulnerability testing.

OHIP also requires access to all system component/solution audit and scan reports and supporting test plans applicable to the system components/solution for which the Contractor was contracted. Examples include, but are not limited to, patch management, change control, vulnerability scanning, Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) application, Security Assessment, Information Security Risk Assessment (ISRA), Third Party Penetration, and Cloud Security and Privacy Compliance reports.

2.3 Additional System Security Privacy Plan Requirements

An SSPP **MUST** be provided by the Contractor for review and approval by the OHIP Security and Privacy Team. The Security and Privacy Team **SHOULD** conduct a formal review process to grade the maturity of the workbook control explanation and supporting artifacts. The SSPP **MUST** reach acceptable maturity scoring levels and **MUST** be approved by Division of Operations and Systems (DOS) Leadership prior to any OHIP data being stored, processed, analyzed, or transmitted by the system.

2.3.1 Control Testing and Effectiveness Assessment

Contractors **MUST** establish a vulnerability management program with automated scanning, regular penetration testing, pre- and post-production application security testing, code analysis, compliance scanning, remediation tracking, and risk assessment.

Contractors **MUST** develop security tests for security and privacy controls, incident response, disaster recovery, social engineering, security awareness, access control, encryption, and continuous monitoring.

OHIP requires Contractors to have an independent, third-party security and privacy assessment performed against the system/solution as part of the process for achieving sign off that the system/solution is ready for go-live from a Security and Privacy compliance perspective.

2.4 Solution Development Life Cycle (SDLC) Change Control

The Security and Privacy team **SHOULD** be included in all phases of the SDLC to provide Security and Privacy compliance input and assessment. The team **MUST** be included in design, development, testing, and deployment phases. In general, all proposed changes that affect the existing System/Solution architecture **MUST** be reviewed and approved by OHIP Leadership. The OHIP Security and Privacy Team requires one hundred and twenty (120) days in advance of making any planned changes to review the proposed change(s) and provide leadership with feedback and recommendation if risks are identified. Documentation provided for architecture/security system change approval **MUST** include details as described in the OHIP Consolidated Technical Change Control Standard's Incident Notifications section.

2.5 Training and Awareness

The Contractor is required to provide comprehensive security and privacy awareness training for all information system users who collect, maintain, store, use, or disclose PII, PHI, PPSI, MCD, FTI, ACA, and SSA data. The training covers, but is not limited to, users' responsibilities for transmitting sensitive information via email, ensuring the proper handling and protection of confidential data.

3.0 Privacy Requirements

The Contractor is responsible for compliance with applicable Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule requirements, State and federal laws and regulations, and OHIP privacy requirements governing protected data. This section describes the OHIP agreements, processes, restrictions, and supporting requirements applicable to Contractor activities involving protected data. Specific Contractor responsibilities, including any required documentation or approvals, are identified within each subsection.

3.1 Data Use Agreement

The DUA is a legally binding agreement between the Department of Health OHIP (the Department) and the requesting Organization to govern the Organization's use and access to MCD. The DUA is used when the Department has determined that the Requestor's stated purpose administers the Medicaid program and complies with the minimum necessary standard established under HIPAA. A Requestor is the person requesting the access to MCD on their own or their organization's behalf. The Requestor is also known as the Authorized Individual.

MCD includes, but is not limited to:

- Names and addresses of Medicaid applicants/recipients.
- Medical services provided.
- Social and economic conditions or circumstances.
- Department of Health evaluation of personal information.
- Medical data, including diagnosis and history of disease or disability.

- Income, eligibility information, and amount of Medicaid payment.
- Information regarding the identification of third parties, and/or information the Department deems to be part of the operations of the Medicaid program that is of a sensitive nature, such as cost of services provided.

Any OHIP data Requestor who has access to, uses, creates, transfers, processes, maintains, transmits, stores **MUST** be pursuant to an executed OHIP DUA. Each element of MCD is confidential regardless of the document, mode of communication, or storage in which it is found.

The Requestor **MAY not** alter the DUA provided by the Department in any way. The individual listed as the Requestor or Authorized Individual **MUST** sign two agreements: the DUA and the BAA. The Custodians **MUST** sign the DUA in Section 4 of the agreement prior to the Requestor signing the DUA. All requirements for Security and Privacy **SHOULD** be passed down to all other vendors or business associates with whom the Requestor shares Medicaid data. The requesting organization agrees to only use the data for the purposes outlined in the DUA or any DUA addendum. The Department retains all ownership rights to the data.

3.2 Data Use Agreement Addendum

The DUA Addendum is used to update the DUA when the Department confirms that requested changes still support Medicaid program operations and comply with HIPAA's minimum necessary requirement. A Names List **MUST** be submitted every quarter with a DUA addendum, even if there are no changes; this is called a Quarterly Names List (QNL) addendum. This ensures that the Custodians review the names list to verify that access to MCD is still appropriate and has not changed for the users listed.

3.3 Names List

A Names List is an Excel file containing the name of each person who has access to MCD on the Lead DUA Organization's behalf. It is a comprehensive record-keeping file that lists any user who has ever had access to MCD, including those working for the Lead DUA Organization, Third Parties, and Downstream Partners. When a user is added to the Names List, they **MUST** remain on the list throughout the life of the DUA.

3.4 Business Associate Agreement (BAA)

MCD **MUST NOT** be shared by the Lead DUA Organization with Business Associates unless the Department accepts a DUA addendum and acknowledges a copy of the BAA executed between the appropriate parties. The BAA **MUST** contain required Third Party Confidentiality Language that is found in the DUA.

Any Business Associate accessing or in direct possession of MCD **MUST** be listed on the DUA Names List with accurate information and effective dates.

3.5 Sensitive Data Types

In addition to PII, PHI, and PPSI, New York State and federal law have specific legal protections for sensitive data types including Substance Use Disorder (SUD), human immunodeficiency virus (HIV)/acquired immunodeficiency syndrome (AIDS), and mental health (MH) data.³

3.6 Use of Production Data Restrictions

The Contractor and any data-consuming entities **MUST NOT** process, store, or transmit confidential, sensitive, or protected data in any preproduction environment. OHIP recognizes that an organization **MAY** have a compelling business need to use such data in a preproduction environment for development, test, and integration purposes. To address this need, the Contractor **MUST**:

- Limit and minimize the amount of data used for internal testing, training, and research purposes.
- Request and obtain DOH authorization before any use of production data for internal testing, training, and research.
- Review and update policies and procedures in accordance with organization-defined frequency.
- Establish and document an anticipated timeline for how long the data will be processed, stored, or transmitted in development, test, and integration environments.⁴
- Verify that the preproduction environment has the same security and privacy controls as would be required in a production environment to safeguard, monitor, and protect the data.

The Contractor **MUST** comply with CMS ARC-AMPE Security Control PM-25 by reviewing and updating, at least annually, policies and procedures addressing the use of data for internal testing, training, and research to ensure continued alignment with evolving requirements.

In support of the authorization requirement above, the Contractor **MUST** document the use case and submit it for OHIP review and approval. The use case documentation **MUST** define:

- The purpose of the request and the proposed use of the data.
- Justification as to why de-identified or synthetic data cannot be used.
- A detailed description of the data being requested.
- The duration for which the data will be retained or accessed.
- How the data will be securely removed or destroyed when no longer needed.

The Contractor **MUST** receive OHIP approval before any production data is used in a preproduction environment. At the conclusion of the effort, OHIP **MAY** require the Contractor to submit a notarized Secure Data Destruction Affidavit Form, signed by a C-Level executive, to OHIP for record keeping.

3.7 De-Identification Restrictions

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of PHI. Under this standard, health information is not individually identifiable if it does not identify an individual and if the

³ Refer to [Appendix C: Legal and Regulatory Compliance](#) in this Standard for more information.

⁴ For additional details and guidance, refer to OHIP Security and Privacy Baseline controls PM-25 and SA-3(2).

covered entity has no reasonable basis to believe it can be used to identify an individual. An organization, and/or covered entity, **MAY** determine that health information is not individually identifiable health information only if a person:

- With appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information is not individually identifiable.
- Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information.
- Documents the methods and results of the analysis that justifies such determination.
- Submits a summary report and supporting documents for OHIP review and acceptance prior to leveraging the de-identified dataset(s).

OHIP data **MUST** remain under the authority of OHIP even after deidentification. The requestor **MAY not** share or disseminate OHIP data without express written consent of OHIP. OHIP also understands that an organization **MAY** have a compelling reason to utilize the Safe Harbor method. To facilitate this potential need, OHIP requires that organizations must:

- Develop, document, and implement policies and procedures that address criteria when Safe Harbor and Expert determination is required, training provided for each method, and or qualifications required for each method.
- Limit or minimize the amount of data used to be de-identified.
- Authorize the use of the de-identified dataset prior to its intended use.
- Review and update policies and procedures in accordance with organization-defined frequency.

In support of the authorization requirement above, the organization **MUST** document the use case for OHIP review and approval, which defines the following:

- Need/Purpose of the request
- Justification regarding why the Safe Harbor method is required when Expert Determination cannot be performed
- Scope of data required
- How long the data is needed
- What will be done with the data, what outputs **MAY** be created, and whether the data will be shared
- How the de-identified data will be securely removed/destroyed when no longer needed

OHIP's approval is required prior to any such use of de-identified datasets. OHIP **MAY** also require a Secure Data Destruction Affidavit form to be completed, signed by a C-Level executive or their authorized representative, notarized, and submitted for OHIP records.

4.0 Zero Trust

Zero Trust is a security strategy used in designing and using the following set of security principles:

- **Verify explicitly:** Always authenticate and authorize based on all available data points.

- **Use least privilege:** Limit user access with just-in-time/Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
- **Assume breach:** Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

These principles are the core of Zero Trust. Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network. Regardless of where the request originates or what resource it accesses, the Zero Trust model teaches us to "never trust, always verify."

Zero Trust is designed to adapt to the complexities of the modern environment that embraces the mobile workforce. Zero Trust protects user accounts, devices, applications, and data wherever they're located. A Zero Trust approach **SHOULD** extend throughout the entire organization and serve as an integrated security philosophy and end-to-end strategy.⁵ The Department adheres to the principles of Zero Trust, and these principles **MUST** be applied throughout the entire solution, unless otherwise determined, at the sole discretion of the Department.

In general:

- Runtime protections **MUST** be applied to all requests and responses that are served by a given architecture, not just at the perimeter. These protections **MUST** be in place whether they originate from exposed services to consumers/partners or used internally within the solution.
- There is no distinction between an "internal" and or an "external" request/response regarding the security protections that are applied to it.

In specific:

- All electronic communication exchanges, whether externally or internally facing, are encrypted end-to-end.
- All end-users are authenticated. The identity of the entity triggering the software to send the request is verified, including a non-person entity (e.g., service account, system account).
- Users with privileged access to system/solution functionality, and/or sensitive data, **MUST** be authenticated with MFA (MFA) credentials. All end-user identities are authorized to access resources. Identities are checked as to whether they **MAY** perform the requested action on a target resource through role-based access control (RBAC).
- The identity of all calling services is verified.
- All calling services are authorized and validated that the action or communication being performed by the service is allowed.

4.1 Encryption

The Department requires that all PPSI be encrypted, both at rest and in transit, in compliance with the current Federal Information Processing Standards (FIPS) 140 series and NYS-S14-007 Encryption standards.

⁵ For more information, refer to the [Zero Trust Overview](#).

The use of the latest versions of Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), Secure Sockets Layer (SSL), and Virtual Private Network (VPN) tunnelling technologies and best practices **SHOULD** be leveraged to further protect the information transmitted over the public internet.

4.2 Identity and Access Management (IAM)

System access or access to sensitive / protected data **MUST** include the use of MFA technology. All identities, including system, admin, and user accounts **MUST** utilize an Identity Provider (IdP) or certificate store that is approved by OHIP. Single-Sign-On (SSO) **MUST** originate from a New York State approved IdP. In addition to this, this standard requires that:

- External facing applications authenticate using the NY.gov IdP.
- State staff users authenticate using NYS Enterprise Single-Sign-On (ESSO) Active Directory, which is integrated with the Medicaid instance of Okta.
- New York State counties, and Local Departments of Social Services (LDSS), shall use the Health Commerce System (HCS) IDP which is integrated with the Medicaid instance of Okta.

If Contractors have more than 20 users (identities), then the Contractor **MAY** utilize their own IdP, if the Contractor IdP can be integrated with the Medicaid Okta instance, and if OHIP provides approval.

OHIP understands that, depending on the use case, exceptions to MFA **MAY** need to be considered. All MFA exception requests **MUST** be documented with detailed justification and provided to OHIP for review and approval by the OHIP Enterprise Architecture and Security and Privacy teams.

4.3 Interface Authorization

Interfaces and endpoints **MUST** verify authorization and content per the Zero Trust Architecture (ZTA) Framework and industry best practices.

- **Identity Management:** All identities, including system, administrator, and user accounts, **MUST** utilize Enterprise-managed identities. Phishing-resistant MFA **SHOULD** be implemented to protect against sophisticated online threats.
- **Identity Governance:** Enterprise user and device accounts, identity records, role assignments, and access attributes **MUST** be created and maintained to support access decisions. This ensures that the right individuals and MES solutions have the appropriate access to the right resources at the right time.
- **Access Control:** Access to resources **MUST** be managed through robust user and device authentication mechanisms (e.g., SSO and MFA). Identity, role, and contextual access attributes **SHOULD** be used to determine and enforce authorization decisions.
- **Federation and Attribute Correlation:** Identity attributes **SHOULD** be aggregated and correlated across systems to support authorization within a ZTA. Federated identity models **SHOULD** be used to allow secure and seamless access across domains, eliminating the need for redundant user administration.
- **Centralized Policy Enforcement and Compliance:** Implement policy-based, centralized, and automated processes to manage identity and access controls. This includes enforcing segregation of duties, managing roles, conducting logging and auditing, performing access reviews, and generating analytics and compliance reports—ensuring adherence to both federal and State regulatory requirements.

4.4 Proper Use of Service Accounts

Each system-to-system integration **MUST** utilize a dedicated non-interactive service account; human user accounts **SHOULD** not be repurposed for these integrations. OHIP reserves the right to review and approve system/service accounts as needed.

When available, use cloud-native mechanisms such as IAM roles or Security Token Service (STS)-issued temporary credentials. If those are unavailable, authentication **MUST** fall back to one of the following:

- 1) OAuth 2.0 Client Credentials Grant
- 2) Mutual Transport Layer Security (mTLS)
- 3) Signed JavaScript Object Notation (JSON) Web Tokens (JWSs) for client authentication as defined in the Request for Comments (RFC) 7523 ("Private Key JWT")
- 4) JWSs signed with a client's private key in accordance with RFC 7521 and RFC 7523

Static credentials **MAY** be used only with explicit approval from the OHIP Security and Privacy Team.

System/Service accounts **SHOULD** be created and provided promptly when requested by OHIP. OHIP reserves the right to define specific SLAs for account provisioning. OHIP reserves the right to request, review, and approve any new service accounts as needed. System/service account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts. System/Service accounts must:

- Disallow all interactive logins (e.g., shell, console, or graphical user interface [GUI]).
- Follow the principle of least privilege.
- Comply with the moderate-baseline controls of NIST SP 800-53.
- Never be used for interactive logins.
- Rotate system/service account credentials regularly, especially if embedded in scripts or apps.
- Notify account managers when an account is created, enabled, modified, disabled, or removed.
- Maintain a registry of all system/service accounts, including their purpose, owner, and access rights.
- Monitor system/service account usage; and
- Report atypical system/service account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

4.5 Secure API Development

Given that APIs have risen to become a primary vector for targeted cyber threats, the Department has created a Secure API Development Baseline to help lower risk associated with unauthorized access and/or use. This Baseline helps protect sensitive data, maintain business continuity, and ensure regulatory compliance based on data classification, and provides a framework for a consistent risk management strategy. The OHIP Secure API Development Baseline provides supporting technical

guidance documents for specifics on the standards and industry best practices. The Department expects that this Baseline **MUST** be followed, as deemed applicable to the specific API use case.

4.6 AI Security and Privacy

The use of AI technology and its rapid deployment in production environments has quickly outpaced industry best practices and strategies for performing risk analysis. The Department has developed an AI Security and Privacy Baseline which defines implementation standards and industry best practices for AI technology. In doing so, this baseline helps mitigate potential ethical and safety risks, safeguards privacy obligations, and establishes a framework for a consistent risk management strategy. Refer to the OHIP AI Security and Privacy Baseline and supporting technical guidance documents for specifics on the standards and industry best practices defined. The Department expects that this Baseline be followed as deemed applicable for specific AI use cases.

4.7 Database Security Requirements

4.7.1 General Database Security

The Contractor **MUST** integrate all databases for authentication with the Department's enterprise IAM solution. After initial deployments, all databases **SHOULD** be integrated with the enterprise IAM solution within 90 calendar days of go-live, with compensating controls documented for any databases requiring extended timelines. The Contractor **MUST NOT** use local database accounts. In scenarios where IAM integration is not possible, the Contractor **MUST** communicate the proposed alternative to the Department for approval. Any approved alternative **MUST** follow the principle of least privilege. The Contractor **MUST** secure all connections to databases. Use of certificates, VPNs, and secured administrative tools is required. The Contractor **MUST** obtain Department approval for access to all databases.

4.7.2 Role-Based Access Control for Databases

The Contractor **MUST** use RBAC for all database users. The Contractor **MUST** establish, define, and utilize appropriate role-based database groups consistently across database environments (e.g., Database Administrator (DBA) role, Developer role, Read Only role). The same role **MUST NOT** be named differently across environments. Access to database objects and data **MUST** be based on the role(s) assigned to the user. Individual user database accounts **MUST** be granted roles, and the roles **MUST** be where the permissions to specific objects and functions are granted. The Contractor **MUST** ensure database users only have access granted in appropriate environments (e.g., developers **MAY** have full object-level permissions only in the development environment, not production). Only users assigned to specific roles **MAY** be allowed access to the database system. Unauthorized access is strictly prohibited.

4.7.3 DBA and Service Account Governance

Only DBAs **MAY** have system-level authorization (DBA role) to manage the overall administration of a database. The Contractor **MUST NOT** grant DBA-level access to users who are not DBAs. System accounts or non-user accounts **MUST NOT** be granted DBA-level access in any database. The Contractor **MUST** ensure all DBAs use individual user accounts, not shared accounts. There **MUST** be traceability for who is performing what actions in the database.

4.7.4 Database Encryption

The Contractor **MUST** encrypt all databases and data in transit and at rest in accordance with the encryption requirements defined in [Section 4.1](#) of this standard.

4.7.5 Database Auditing and Logging

The Contractor **MUST** implement the following database auditing requirements:

- **Auditing Data Changes:** The Contractor **MUST** build tracking of how data is selected, inserted, updated, and deleted into the database design. Fields or tables that register when a record was created, updated, or deleted and by whom **MUST** be integrated. Standard practices such as 'last_update_date' and 'create_date' columns **MAY** address these requirements if approved by the Department.
- **Auditing Database Modifications:** The Contractor **MUST** monitor changes to the database design, structure, or configuration through the Relational Database Management System (RDBMS) logging and auditing configuration.
- **Connection Logging:** The Contractor **MUST** activate database connection logging. Connection logs **MUST** include who (user or system account), when (timestamp), from where (IP address or application name), and what database and objects were accessed.

5.0 Enterprise Security Architecture

Contractor design **SHOULD** incorporate security best practices where possible in protecting the solution and data contained within. The list below highlights some examples, but not all, of industry best practices.

- Three-tier architecture **SHOULD** include Web Application firewalls, load balancers, and Demilitarized Zones (DMZ) as deemed necessary. Application service **MUST** be hardened and locked down to minimum necessary to with the web firewall and backend database server, and Database (DB) Servers **SHOULD** be locked down to only allow minimum communication with the app servers and locked down to allow database administration and management support. Network segmentation **SHOULD** include a firewall and Data Loss Protection (DLP) monitoring and alerting between security zones. Where possible, a subnet **SHOULD** be in place.
- Minimum necessary services, protocols, ports, and applications installed on all system components **MUST** be defined and maintained. These secured baselines **MUST** be monitored continuously and alerting thresholds defined when indicators of compromise or threats are detected.
- In addition, host-based protections, such as firewall, DLP, Anti-virus, and Intrusion Protection and Detections, **SHOULD** be leveraged to ensure continuous monitoring and alerting protections are in place.

5.1 Comingling Restrictions

Restricting the comingling of data between consumers in a cloud environment is crucial for maintaining data privacy, security, and compliance. The goal is to make sure that the data is properly isolated, and access is limited to authorized users Here are several standards and practices that can help achieve this:

- **Trusted Principle Identification:**
 - o Comply with the Zero Trust, IAM section of this standard

- **Verified Principal Permissions:**
 - o Verified permissions provides authorization by verifying whether a principal is allowed to perform an action on a resource in a given context in the application.
 - o Permissions **SHOULD** minimally be verified in both the user experience (UX) and APIs.
 - o Comply with the Zero Trust Interface Authorization section of this standard.
- **Resource (Data) Ownership:**
 - o Implement a structure where data is stored in a manner that isolates records associated with different owners. This can be achieved through database schemas, partitions, or virtual private configurations.
 - o For all resources, it **MUST** be possible to determine ownership and any delegated permissions, regardless of the access path.
 - o Where encryption can be utilized as a control on data access (e.g., private data encrypted with a consumer-owned key), it **MUST** be used.
- **Architecture Isolation:**
 - o Use virtual network segmentation to isolate traffic between different consumer environments, reducing the risk of data comingling through network vulnerabilities.
 - o Use logical separation of consumer data through virtualization technologies to ensure that data from different consumers does not mix.
 - o Implement data masking or anonymization techniques for sensitive data used in non-production environments or as needed for compliance with privacy regulations.
 - o Implement tenant isolation at the application level, ensuring that data access is strictly controlled based on consumer IDs or tenant identifiers.

6.0 Cloud Security

6.1 Federal Risk and Authorization Management Program (FedRAMP) Authorization

When leveraging a cloud environment, it **MUST** minimally be FedRAMP authorized at the moderate impact level.

6.2 Contractor Cloud Compliance

Contractors **MUST** enable all security settings and features for cloud-deployed products as recommended by product literature (or documentation). Any necessary adjustments or deactivation of security settings to accommodate business functionality **MUST** be reviewed, approved, and documented by the Privacy and Security Department. A compensating control **SHOULD** be identified in lieu of deactivation.

When a cloud service, used by Contractors, faces the inability to apply a prescribed security control due to technical, operational, or contractual constraints, simply deactivating the service could disrupt operations or negate its benefits. Instead, organizations **SHOULD** identify compensating controls as an alternative measure to effectively manage and mitigate risks.

Compensating controls are security solutions or practices designed to achieve the intended security posture of the original control. These controls **SHOULD** be thoughtfully selected and tailored based on

the risk assessment, ensuring they provide a level of security that aligns with the original compliance requirement.

6.3 Automated Compliance Cloud Tools

Where the cloud or technology provides automated governance compliance monitoring, the Contractor **SHOULD** present recommendations for automated governance compliance monitoring features to OHIP for joint evaluation and cost-benefit analysis. Given that there is often a cost associated with doing so, these recommendations **MUST** be reviewed and approved by the Privacy and Security Department prior to OHIP sign off.⁶

Contractors **MUST** establish a process, approved by OHIP, to report vendor-automated compliance findings to the OHIP Security and Privacy Team and address any issues identified.

6.4 Onshore Compliance

Contractors **MUST** comply with the following requirements below relative to location of staff and data:

- All data **MUST** physically reside within the United States and its territories.
- All access and support staff **MUST** also be located within the United States. No offshore access or processing of the solution or data contained within is permitted.⁷

6.5 Software-as-a-Service (SaaS)

Any Commercial Off-the-Shelf (COTS) solution, including SaaS offerings, **MUST** comply with the security and privacy control standards baseline for the protection of the application and of all sensitive or confidential information stored, accessed, or processed by the solution.

Where a Contractor's solution leverages SaaS offerings, the Contractor **MUST** ensure that the SaaS offering meets all applicable security and privacy standards. Every SaaS solution **MUST** implement security controls appropriate to the classification of the data in question, based on NYS-S14-002 New York State Information Classification Standard. Applicable security and privacy standards include:

- CMS ARS
- ARC AMPE
- IRS Publication 1075
- SSA TSSR

The Contractor **MAY** demonstrate compliance with these standards through one of the following methods, or through another means approved by OHIP, provided the chosen method verifies that the required controls are implemented correctly, operating as intended, and producing the desired outcome:

- FedRAMP Authorization.
- CMS Authority to Operate (ATO) or Authority to Connect (ATC).

⁶ For more information, refer to the OHIP Infrastructure and Operations Domain Document, Cloud FinOps Standard.

⁷ For more information, refer to the OHIP Offshoring Data Policy.

- Health Information Trust Alliance (HITRUST) r2 certification scoped for the SaaS solution which includes the NY Security Regulatory Risk factor.
- A NIST control assessment performed by a qualified third-party cloud security and privacy assessor engaged by the Contractor.

The Contractor **MUST** provide OHIP with a client responsibility matrix (CRM) for the SaaS solution that identifies where control responsibility is solely owned and where responsibilities are shared between the SaaS provider and its clients.

7.0 Logging and Continuous Monitoring

7.1 Continuous Security Operations

All MES solutions containing MCD **MUST** establish an around-the-clock (twenty-four [24] hours, seven [7] days a week) Security Operations Center to provide continuous monitoring, detection, and response capabilities for security-related events and incidents.

7.2 Security Information and Event Management (SIEM)

All MES solutions **MUST** have a robust SIEM solution to collect, analyze, and correlate security-related logs and events from various systems and applications, enabling OHIP to detect and respond to security incidents and threats effectively. This **SHOULD** include logs and reports of user access to all sensitive data, what records they accessed along with date and time of access.

8.0 Certification and Operational Compliance

8.1 Framework and Processes

Where deemed applicable, the Contractors **MUST** implement comprehensive frameworks and processes to comply with all federal certification requirements such as, but not limited to, the ATO or ATC. These certifications typically apply when the solution needs to connect directly with CMS or when FTI or SSA information is stored/accessed in the solution being built on behalf of the Department.

It is also expected that the Contractor maintains ongoing compliance with applicable State and federal regulations and standards. This framework **MUST** address both initial certification activities and continuous compliance monitoring throughout the program life cycle.

This framework **MUST** include, but is not limited to, establishing systematic processes for evaluating certification requirements and planning appropriate implementation approaches. These processes **MUST** incorporate technical and operational considerations while aligning with Department objectives and State and federal Laws and policies.

8.2 Certification Support

Contractors **MUST** provide comprehensive support for achieving and maintaining CMS, IRS, and SSA audit, compliance, and certification requirements for all applicable MES components throughout the program life cycle. This support **MUST** include detailed planning and execution of all certification activities while ensuring appropriate documentation of compliance evidence.

The Contractor **SHOULD** develop and maintain detailed certification tracking mechanisms that monitor progress toward certification milestones and provide clear visibility into certification status. These

mechanisms **MUST** provide clear visibility into certification status while enabling early identification of potential compliance issues. The tracking system **MUST** maintain comprehensive documentation of all certification evidence and related communications.

8.3 Asset Management and System Inventory

Contractors are required to:

- Perform an inventory to identify all critical information system assets, which includes hardware, software, firmware, information, data, applications, communications, and personnel to support essential missions and business functions.
- Ensure that critical system assets are tightly integrated with the primary system Disaster Recovery/Business Continuity Plan.
- Run automated mechanisms as part of the Continuous Monitoring Program to collect hardware and software configuration data. Examples of automated mechanisms include, but are not limited to:
 - o Hardware asset management systems
 - o Software asset management systems
 - o Centralized configuration management software
- Comply with the control requirements as defined OHIP Security and Privacy Baseline control "CM-8 System Component Inventory."

The Department expects, at a minimum, an annual System Component Inventory listing all hardware and software licenses associated with the solution managed and supported. The Department will provide guidance on what information will be required, define the format of these annual reports, and the method in which to securely submit. The Department reserves the right to request the current inventory reports as needed.

8.4 System/Solution Audit Support and Management

Contractors **MUST** establish comprehensive processes for supporting internal and independent third-party audits associated with Security and Privacy control implementations. These processes **MUST** provide systematic approaches for preparing audit documentation while ensuring appropriate responses to audit findings.

Contractors **MUST** maintain detailed tracking of all audit activities, including findings, remediation plans, and verification of corrective actions. This tracking **MUST** support immediate audit response needs and longer-term compliance improvement efforts.

8.5 Vulnerability Scanning and Reporting

In compliance with Department policy and federal requirements, the Contractor **MUST** perform routine vulnerability scans against the system or system components to identify where vulnerabilities exist and manage remediating them or incorporating compensating controls in place to lower risk to acceptable levels when remediation is not possible. Multiple scan types **SHOULD** be performed where applicable (e.g., Web, Operating System [OS], Network, and application). The Department reserves the right to perform their own "trust but verify", OS, and/or network testing as deemed necessary.

8.6 Application Security Testing and Reporting

The Contractor **MUST** provide access to SAST, DAST, and the findings reports. The Security and Privacy Department requires access to review and approve test plans. The Department reserves the right to perform their own “trust but verify” application/web application testing as deemed necessary.

8.7 Penetration Testing and Reporting

The Contractor **SHOULD** allow previews of actual Penetration Test Plan and Findings Reports prior to final submission. The Contractor **MUST** deliver all final Penetration Test Plans and Findings Reports to OHIP. The type of penetration testing is determined by use case. Testing can include, but is not limited to, internal, external/internet, anonymous, and/or authenticated, network and or application. OHIP reserves the right to perform their own “trust but verify” penetration testing.

8.8 Incident Management and Reporting

Contractors **MUST** tightly integrate their Incident Management process with existing OHIP incident management procedures. All security and privacy events, and suspected events, **MUST** be reported to the Security and Privacy incident report mailbox: IncidentReport@health.ny.gov AND the Security and Privacy program support mailbox: doh.sm.Medicaid.Data.Exchange@health.ny.gov within one hour of discovery.

Furthermore, the Contractor must:

- Promptly investigate and report the vendor’s determinations regarding any alleged or actual unauthorized use, reuse, or disclosure of OHIP data to OHIP.
- Promptly resolve any issues identified by the investigation.
- Submit a CAP with steps designed to prevent any future unauthorized uses, reuses, or disclosures.
- Work with OHIP Security and Privacy to complete and return all requested forms in a timely manner.

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 Standard. This table captures the lifecycle of the domain document from initial publication onward.

Date	Version	Author	Description of Change
------	---------	--------	-----------------------

07/10/25	1.0	NYS TAS	Initial draft.
09/18/25	1.1	Security and Privacy	Re-written to better align with Department operating procedures.
11/12/25	1.2	Randy Wheeler	Standard approved.
12/11/25	1.3	NYS TAS	Updated the name and description of the System Component Inventory Deliverable; added Federal Trade Commission Health Breach Notification Rule and New York State Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) to Appendix B.
01/05/26	1.4	Security and Privacy, NYS TAS	Updated Section 4.2 Identity and Access Management. Revised the following deliverable and artifact descriptions: System Security and Privacy Plan, Information Security Risk Assessment, Penetration Test Plan and Findings Report, and the Continuous Monitoring Plan.
6/10/26	1.5	Security and Privacy, NYS TAS	Updated Section 1.0 for Compliance Tier Framework, and new sections 3.6 and 6.5
10/23/26	1.6	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 5 – Deliverables and Artifacts

Type	Name	Definition
Deliverable	Continuous Monitoring Plan (CMP)	<p>A Continuous Monitoring Plan (CMP) is designed to ensure ongoing security and privacy compliance by identifying, assessing, and mitigating risks in real time. This plan enables proactive management of potential threats and vulnerabilities. Components of the CMP include, but are not limited to:</p> <ul style="list-style-type: none"> • <i>Risk Assessment Methodology</i>—Outline the processes for identifying and evaluating risks associated with system operations • <i>Monitoring Tools and Technologies</i>—Specify the tools and technologies to be used for continuous system monitoring • <i>Data Collection and Analysis</i>—Describe methods for collecting and analyzing security data to detect anomalies or threats • <i>Incident Response Procedures</i>—Describe protocols for responding to identified incidents or security breaches • <i>Reporting and Documentation</i>—Define how findings will be documented and reported to stakeholders • <i>Roles and Responsibilities</i>—Detail the roles and responsibilities of team members involved in the continuous monitoring process • <i>Frequency of Monitoring Activities</i>—State the frequency at which monitoring activities and assessments will occur • <i>Compliance Requirements</i>—List relevant compliance frameworks and standards the plan adheres to • <i>Change Control Process</i>—Explain the process for updating the monitoring plan in response to changes in technology, regulation, or threat landscape

Deliverable	Corrective Action Plan	<p>A Corrective Action Plan (CAP) is a strategic document used to identify, address, and resolve issues that do not meet the desired standards or contractual obligations. The purpose of a CAP remains consistent across different domains. However, its application can vary depending on the specific context. Contractors are expected to submit Corrective Action Plan(s) as part of any Incident Management Process. The Plan must include, but not be limited to:</p> <ul style="list-style-type: none"> • <i>Issue Identification</i>—Description of the problem or non-compliance issue being addressed, including its scope and impact • <i>Root Cause Analysis</i>—Examination of the underlying causes of the issue to prevent recurrence, including contributing factors • <i>Action Steps</i>—Specific activities and measures to be implemented to correct the identified issues, including timelines and milestones • <i>Responsibility Assignment</i>—Designation of roles and responsible parties for executing and overseeing the corrective measures • <i>Metrics for Success</i>—Criteria and indicators used to measure the effectiveness and completion of corrective actions • <i>Monitoring and Evaluation</i>—Procedures for tracking progress and assessing the success of the corrective actions over time • <i>Review and Approval Process</i>—Protocol for reviewing the proposed corrective actions and obtaining necessary approvals from stakeholders • <i>Communication Strategy</i>—Plans for communicating updates and outcomes to relevant parties, including documentation and reporting formats • <i>Risk Assessment</i>—Evaluation of potential risks associated with the corrective actions, including mitigation strategies <p>The Department reserves the right to indicate the templates and/or processes for the submission of the Corrective Action Plan.</p>
Deliverable	Information Security and Privacy Compliance Audit	<p>The Information Security and Privacy Compliance Audit examines the security postures and practices of the solution. The audit scrutinizes the effectiveness of physical and digital security measures, alignment of security policies and procedures with standards and regulatory requirements, and adequacy of incident responses and the BCDR Plan.</p>

Deliverable	Information Security Risk Assessment (ISRA)	The ISRA is a document or documents to communicate the results of an Information Security Risk Assessment. This is not to be confused with the assessment itself. An Information Security Risk Assessment is an evaluation of the potential vulnerabilities and threats per NIST 800-115, NIST 800-30, and OHIP Security and Privacy Standards that could affect the confidentiality, integrity, and availability of the information assets. The assessment includes identifying sensitive data, critical system components, potential risks, and the potential impact of security breaches. The ISRA provides the results of the assessment to the Department and must include preventative strategies to address identified or reported vulnerabilities and threats. The POA&M must document, track, and address any open items identified in the ISRA.
Deliverable	Plan of Action and Milestones (POA&M)	The POA&M addresses deficient controls in the SSPP and SSPP Workbook and must provide target implementation dates for any control not fully implemented. Deficient controls must be prioritized and mitigated with compensating controls consistent with federal and state policies and standards. The Contractor must update and resubmit the POA&M to the Department each quarter throughout the term of the Contract to demonstrate progress and assure mitigation of deficient security controls and any third-party assessor findings. The Department reserves the right to require the Contractor to retain, at the Contractor's expense, a third-party firm to perform additional security assessments at any time.

Deliverable	Penetration Test Plan and Findings Report	<p>A Penetration Test Plan and Findings Report assesses the security posture of systems and applications. The Penetration Test Plan outlines the methodology and scope of the testing, while the Findings Report documents the outcomes, including vulnerabilities identified and recommended remediation actions. Together, these documents provide a comprehensive view of the organization's security posture and guide improvements for safeguarding sensitive data and systems.</p> <ul style="list-style-type: none"> • <i>Testing Personnel</i> – Describes the personnel, their qualifications, credentials, and experience, as well as their contact information in case the Department needs to reach them during the test • <i>Test Objectives</i>—Description of the goals of the penetration testing, including specific security aspects to be assessed • <i>Scope Definition</i>—Clear delineation of systems, networks, and applications that will be tested, alongside exclusions, if any • <i>Testing Methodology</i>—Outline of the approach and techniques to be used in the penetration testing, including tools and frameworks • <i>Risk Assessment</i> – Identification of potential risks associated with testing, including impact on systems and data, and mitigation strategies • <i>Pre-Engagement Briefing</i>—Description of preparatory activities, including stakeholder meetings and setting expectations • <i>Execution Timeline</i>—Schedule for testing activities, specifying key phases and duration • <i>Findings</i> – <ul style="list-style-type: none"> o <i>Executive Summary</i>—Concise overview of the testing outcomes, highlighting key findings and overall security posture o <i>Detailed Findings</i>—Comprehensive documentation of vulnerabilities discovered, categorized by severity, and including detailed descriptions o <i>Impact Analysis</i>—Assessment of potential impacts of identified vulnerabilities on business operations and data integrity o <i>Recommendations</i>—Suggested remediation actions to address vulnerabilities, including prioritization and estimated effort o <i>Evidence and Supporting Data</i>—Collection of logs, screenshots, and other documentation that substantiates findings o <i>Post-Test Debrief</i>—Summary of post-testing activities, including stakeholder engagement and discussions on findings and next steps o <i>Supporting Documentation</i>—Any supporting documentation completed in support of the Penetration Test Plan and Findings Report (e.g., scan results), as requested by the Department
-------------	---	--

Deliverable	System Component Inventory	The System Component Inventory deliverable is a listing of all managed and supported hardware and software licenses associated with the system. This deliverable is typically provided annually.
Deliverable	System Security and Privacy Briefing	The System Security and Privacy Briefing provides an overview of the solution's security policies, protocols, and requirements. The briefing must include a review of the relevant federal and state regulations that govern data protection and privacy, such as HIPAA for health care information and NIST/FISMA for federal data security. It covers the specific security measures and technologies in place for the solution.
Deliverable	System Security and Privacy Plan	<p>The System Security and Privacy Plan enables the Contractor to demonstrate compliance with the OHIP Security and Privacy Compliance Standard. It must include, but not be limited to:</p> <ul style="list-style-type: none"> • <i>Systems Scope and Summary</i>—Systems are in scope (e.g., eligibility, billing, provider management, etc.) and outline any out-of-scope areas or transitional exceptions • <i>Location of Repository for Security Documentation</i>—Provide the location and a brief description of the repository's structure for contractor security artifacts, for both draft and final documentation • <i>Timeline and Milestones</i>—Outline high-level phases (design, authoring, submissions) with target dates, and list key milestones including Security and Privacy Team checkpoints • <i>Roles and Responsibilities</i>—Describe key roles and responsibilities of implementation team members • <i>Security and Privacy Risk Assessment Methods</i>—Describe the security testing methodology, including how and where security testing will be implemented to meet the security requirements • <i>Security and Privacy Compliance Tools</i>—List all security and privacy compliance services and tools to be used in support of the proposed solution • <i>Identity Providers (IdP)</i>—List all identity providers and certificate stores intended to be used in support of the proposed solution • <i>Data Use Agreements (DUAs) and Business Associate Agreements (BAAs)</i>—List all applicable DUA and BAAs to be executed in support of the proposed solution • <i>Security Reporting and Metrics</i>—List all compliance reporting and metrics and their frequency • <i>Risk and Mitigation</i>—Describe the approach to identify, report, and mitigate risks • <i>Assumptions, Constraints, and Dependencies</i>—Describe any assumptions, constraints, and dependencies that may impact security and privacy compliance

Deliverable	System Security and Privacy Plan Workbook	<p>The System Security and Privacy Plan Workbook enables Contractors to detail, track, and document adherence to the SSPP. In the workbook, the Contractor must fully explain and document how the security control and risk management requirements will be implemented. In addition, the Contractor must implement and maintain all security controls and risk management processes. The security controls must be organized into families for ease of use in the control selection and specification process. There are eighteen (18) security control families from NIST 800-53, and additional safeguards required by Internal Revenue Code (IRC) § 6103(p)(4), as defined by Publication 1075 (Tax Information Security Guidelines, for Federal, State and Local Agencies), for FTI. Each family contains security controls related to the security functionality of the family. Controls common to both CMS and IRS requirements are documented in the SSPP Workbook. Controls specific to the protection of FTI or controls above the common controls must also be documented. The Contractor must update and maintain the SSPP Workbook to meet CMS, NIST, and IRS security controls.</p>
Artifact	Security Incident Report	<p>The Security Incident Report contains an account of any security incident, including the date, time, and location of the occurrence. This report must be submitted after a security incident and outline the nature and scope of the incident, identifying specifically what part of the solution was affected, the potential data compromised, and the initial impact assessment. The Department reserves the right to dictate the templates and/or processes for the submission of the Security Incident Report.</p>

Appendix B: Master Requirements Summary

The following table consolidates all 98 requirements from this domain standard with individual RFC 2119.

Table 6 – Master Requirements Summary Table

Req. ID	Requirement Statement	Tier	Standard Section
Security and Privacy Compliance Standard SEC-0001 to SEC-0098 98 Requirements: MUST 82 SHOULD 16 MAY 0			
SEC-0001	The CMS ARS Security and Privacy Control Baseline MUST be followed for all MES systems containing MCD.	MUST	2.1 – Additional Data Classifications
SEC-0002	If applicable, the CMS ARC-AMPE Security and Privacy Control Baseline MUST be followed for ACA data. OHIP has developed an ACA Overlay Control workbook to include additional controls.	MUST	2.1 – Additional Data Classifications
SEC-0003	If applicable, the IRS Publication 1075 Security and Privacy Control Baseline MUST be followed for FTI data. OHIP has developed an FTI Overlay Control workbook to include additional controls.	MUST	2.1 – Additional Data Classifications
SEC-0004	If applicable, the SSA TSSR Security and Privacy Control Baseline MUST be followed for SSA data. OHIP has developed an SSA Overlay Control workbook to include additional controls.	MUST	2.1 – Additional Data Classifications
SEC-0005	The Contractor MUST demonstrate compliance with the SSPP through completion of SSPP workbooks, HITRUST certification with NYS Regulatory Risk factor, or other OHIP-approved methods.	MUST	2.2 – System Security and Privacy Plan
SEC-0006	The Contractor MUST complete the SSPP workbooks and any additional applicable data classification workbook overlays, explaining in detail how each control is implemented.	MUST	2.2 – System Security and Privacy Plan
SEC-0007	OHIP reserves the right to independently test and verify security and privacy controls. The Contractor MUST provide OHIP access to Acceptance Testing infrastructure and Production for verification.	MUST	2.2 – System Security and Privacy Plan
SEC-0008	The Contractor MUST provide an SSPP for review and approval by the OHIP Security and Privacy Team.	MUST	2.2 – System Security and Privacy Plan
SEC-0009	The Security and Privacy Team SHOULD conduct a formal review process to grade the maturity of the workbook control explanation and supporting artifacts.	SHOULD	2.2 – System Security and Privacy Plan
SEC-0010	The Contractor MUST establish a vulnerability management program with automated scanning, regular penetration testing, pre- and post-production application security testing, code analysis, and compliance scanning.	MUST	2.3.1 Control Testing

SEC-0011	The Contractor MUST develop security tests for security and privacy controls, incident response, disaster recovery, social engineering, security awareness, access control, encryption, and continuous monitoring.	MUST	2.3.1 Control Testing
SEC-0012	The Security and Privacy team SHOULD be included in all phases of the SDLC to provide Security and Privacy compliance input and assessment. The team MUST be included in design, development, testing, and deployment phases..	SHOULD	2.4 – SDLC Change Control
SEC-0013	The Contractor MUST provide comprehensive security and privacy awareness training for all information system users who collect, maintain, store, use, or disclose PII, PHI, PPSI, MCD, FTI, ACA, or SSA data.	MUST	2.5 – Training and Awareness
SEC-0014	Any OHIP data Requestor who has access to, uses, creates, transfers, processes, maintains, transmits, or stores MCD MUST do so pursuant to an executed OHIP DUA.	MUST	3.1 – Data Use Agreement
SEC-0015	The Requestor MUST NOT alter the DUA provided by the Department. The Requestor or Authorized Individual MUST sign both the DUA and the Business Associate Agreement.	MUST	3.1 – Data Use Agreement
SEC-0016	The DUA Addendum MUST be used to update the DUA when requested changes still support Medicaid program operations and comply with HIPAA minimum necessary standards.	MUST	3.2 – DUA Addendum
SEC-0017	The Lead DUA Organization MUST maintain a Names List containing every person who has access to MCD, updated within five business days of any personnel change.	MUST	3.3 – Names List
SEC-0018	MCD MUST NOT be shared with Business Associates unless the Department accepts a DUA addendum and acknowledges a copy of the executed BAA.	MUST	3.4 – Business Associate Agreement
SEC-0019	Any Business Associate accessing or in direct possession of MCD MUST be listed on the DUA Names List with accurate information and effective dates.	MUST	3.4 – Business Associate Agreement
SEC-0020	The Contractor MUST NOT process, store, or transmit confidential, sensitive, or protected data in any preproduction environment without OHIP authorization.	MUST	3.6 – Production Data Restrictions
SEC-0021	The Contractor MUST request and obtain DOH authorization before any use of production data for internal testing, training, and research.	MUST	3.6 – Production Data Restrictions
SEC-0022	The Contractor MUST verify that preproduction environments have the same security and privacy controls as production environments.	MUST	3.6 – Production Data Restrictions
SEC-0023	The Contractor MUST receive OHIP approval prior to any production data being used in a preproduction environment.	MUST	3.6 – Production Data Restrictions
SEC-0024	The Contractor MUST document the use case for production data use including: purpose, justification why de-identified/synthetic data cannot be used, data description, retention duration, and secure destruction plan.	MUST	3.6 – Production Data Restrictions

SEC-0025	The Contractor MUST comply with CMS ARC-AMPE Security Control PM-25 by reviewing and updating, at least annually, policies and procedures addressing the use of data for internal testing, training, and research to ensure continued alignment with evolving requirements.	MUST	3.6 – Production Data Restrictions
SEC-0026	The Contractor MUST limit and minimize the amount of data used for internal testing, training, and research purposes.	MUST	3.6 – Production Data Restrictions
SEC-0027	OHIP data MUST remain under the authority of OHIP even after de-identification. The requestor MUST NOT share or disseminate OHIP data without express written consent.	MUST	3.7 – De-Identification
SEC-0028	The Contractor MUST develop, document, and implement policies and procedures addressing criteria for Safe Harbor and Expert Determination methods.	MUST	3.7 – De-Identification
SEC-0029	The Contractor MUST document the use case for OHIP review and approval before using de-identified datasets, including: need/purpose, justification, scope, duration, outputs, and destruction plan.	MUST	3.7 – De-Identification
SEC-0030	OHIP approval MUST be obtained prior to any use of de-identified datasets.	MUST	3.7 – De-Identification
SEC-0031	Runtime protections MUST be applied to all requests and responses served by a given architecture, not just at the perimeter.	MUST	4.0 – Zero Trust – General
SEC-0032	All electronic communication exchanges, whether externally or internally facing, MUST be encrypted end-to-end.	MUST	4.0 – Zero Trust – General
SEC-0033	All end-users MUST be authenticated. The identity of the entity triggering the software to send the request MUST be verified, including non-person entities.	MUST	4.0 – Zero Trust – General
SEC-0034	Users with privileged access MUST be authenticated with multi-factor authentication (MFA) credentials.	MUST	4.0 – Zero Trust – General
SEC-0035	All PPSI MUST be encrypted, both at rest and in transit, in compliance with the current FIPS 140 series and NYS encryption standards.	MUST	4.1 – Encryption
SEC-0036	The Contractor SHOULD use the latest versions of HTTPS, SFTP, SSL, and VPN tunnelling technologies for data in transit.	SHOULD	4.1 – Encryption
SEC-0037	System access or access to sensitive/protected data MUST include the use of Multi-factor Authentication technology.	MUST	4.2 – Identity and Access Management
SEC-0038	All identities, including system, admin, and user accounts MUST utilize an Identity Provider (IdP) integrated with the DOH Medicaid Okta instance.	MUST	4.2 – Identity and Access Management
SEC-0039	NYS counties and LDSS MUST use HCS IDP integrated with the Medicaid instance of Okta.	MUST	4.2 – Identity and Access Management
SEC-0040	All MFA exception requests MUST be documented with detailed justification and provided to OHIP for review and approval.	MUST	4.2 – Identity and Access Management

SEC-0041	Interfaces and endpoints MUST verify authorization and content per the Zero Trust Architecture Framework and industry best practices.	MUST	4.3 – Interface Authorization
SEC-0042	All identities MUST utilize Enterprise-managed identities. Phishing-resistant MFA SHOULD be implemented.	MUST	4.3 – Interface Authorization
SEC-0043	Enterprise user and device accounts, identity records, role assignments, and access attributes MUST be created and maintained to support access decisions.	MUST	4.3 – Interface Authorization
SEC-0044	Access to resources MUST be managed through robust user and device authentication mechanisms (e.g., SSO and MFA).	MUST	4.3 – Interface Authorization
SEC-0045	Identity attributes SHOULD be aggregated and correlated across systems to support authorization within a Zero Trust Architecture.	SHOULD	4.3 – Interface Authorization
SEC-0046	Each system-to-system integration MUST utilize a dedicated non-interactive service account; human user accounts MUST NOT be repurposed for integrations.	MUST	4.4 – Service Accounts
SEC-0047	When available, cloud-native mechanisms (IAM roles or STS-issued temporary credentials) MUST be used. If unavailable, authentication MUST use OAuth 2.0, mTLS, or signed JWTs.	MUST	4.4 – Service Accounts
SEC-0048	Static credentials MAY be used only with explicit approval from the OHIP Security and Privacy Team.	SHOULD	4.4 – Service Accounts
SEC-0049	System/Service accounts SHOULD be created and provided promptly when requested by OHIP. OHIP reserves the right to define specific SLAs for account provisioning.	SHOULD	4.4 – Service Accounts
SEC-0050	System/Service accounts MUST : disallow all interactive logins, follow least privilege, comply with NIST SP 800-53 moderate-baseline controls, rotate credentials regularly, and maintain a registry of all accounts.	MUST	4.4 – Service Accounts
SEC-0051	The Contractor MUST comply with the OHIP Secure API Development Baseline for all API development and integration work.	MUST	4.5 – Secure API Development
SEC-0052	The Contractor SHOULD comply with the OHIP AI Security and Privacy Baseline for any use of AI technology in the MES environment. Where OHIP deems a specific AI use case applicable, compliance with the Baseline becomes mandatory	SHOULD	4.6 – AI Security and Privacy
SEC-0053	The Contractor MUST integrate all databases for authentication with the Department's enterprise IAM solution.	MUST	4.71 – General Database Security
SEC-0054	After initial deployments, all databases SHOULD be integrated with the enterprise IAM solution within 90 calendar days of go-live, with compensating controls documented for any databases requiring extended timelines.	SHOULD	4.71 – General Database Security
SEC-0055	The Contractor MUST use Role-Based Access Control (RBAC) for all database users.	MUST	4.7.2 – Database RBAC

SEC-0056	The Contractor MUST establish, define, and utilize appropriate role-based database groups consistently across database instances.	MUST	4.7.2 – Database RBAC
SEC-0057	The Contractor MUST NOT grant DBA-level access to users who are not database administrators.	MUST	4.7.3 – DBA and Service Account Gov
SEC-0058	DBA activities MUST be logged and auditable. Access reviews MUST be conducted at a frequency approved by OHIP.	MUST	4.7.3 – DBA and Service Account Gov
SEC-0059	The Contractor MUST encrypt all databases and data in transit and at rest per Section 4.1 encryption requirements.	MUST	4.7.4 – Database Encryption
SEC-0060	The Contractor MUST build tracking of how data is selected, inserted, updated, and deleted into the database design.	MUST	4.7.5 – Database Auditing
SEC-0061	The Contractor MUST monitor changes to database design, structure, or configuration through RDBMS logging and auditing.	MUST	4.7.5 – Database Auditing
SEC-0062	The Contractor MUST activate database connection logging including who, when, from where, and success/failure status.	MUST	4.7.5 – Database Auditing
SEC-0063	Application services MUST be hardened and locked down to minimum necessary.	MUST	5.0 – Enterprise Security Arch
SEC-0064	Minimum necessary services, protocols, ports, and applications MUST be defined and maintained with secured baselines continuously monitored.	MUST	5.0 – Enterprise Security Arch
SEC-0065	Three-tier architecture SHOULD include Web Application firewalls, load balancers, and DMZ as deemed necessary.	SHOULD	5.0 – Enterprise Security Arch
SEC-0066	Host-based protections (firewall, DLP, Anti-virus, IPS/IDS) SHOULD be leveraged for continuous monitoring and alerting.	SHOULD	5.0 – Enterprise Security Arch
SEC-0067	For all resources, it MUST be possible to determine ownership and any delegated permissions, regardless of the access path.	MUST	5.1 – Comingling Restrictions
SEC-0068	Where encryption can be utilized as a control on data access, it MUST be used.	MUST	5.1 – Comingling Restrictions
SEC-0069	Permissions SHOULD minimally be verified in both the UX and APIs.	SHOULD	5.1 – Comingling Restrictions
SEC-0070	When leveraging a cloud environment, it MUST minimally be FedRAMP authorized at the moderate impact level.	MUST	6.1 – FedRAMP Authorization
SEC-0071	The Contractor MUST enable all security settings and features for cloud-deployed products as recommended by product documentation.	MUST	6.2 – Cloud Compliance
SEC-0072	Deactivation of security settings MUST be documented, justified, and approved by OHIP.	MUST	6.2 – Cloud Compliance
SEC-0073	When a control cannot be applied, compensating controls SHOULD be implemented to achieve equivalent security posture.	SHOULD	6.2 – Cloud Compliance

SEC-0074	The Contractor SHOULD present recommendations for automated governance compliance monitoring features to OHIP for joint evaluation and cost-benefit analysis.	SHOULD	6.3 – Automated Compliance Tools
SEC-0075	The Contractor MUST establish an OHIP-approved process to report vendor-automated compliance findings and address identified issues.	MUST	6.3 – Automated Compliance Tools
SEC-0076	All data MUST physically reside within the United States and its territories.	MUST	6.4 – Onshore Compliance
SEC-0077	All access and support staff MUST be located within the United States. No offshore access or processing is permitted.	MUST	6.4 – Onshore Compliance
SEC-0078	Any COTS solution, including SaaS offerings, MUST comply with the security and privacy control standards baseline for application protection and for all sensitive or confidential data stored, accessed, or processed, with security controls appropriate to the classification of the data per NYS-S14-002.	MUST	6.5 – SaaS
SEC-0079	The Contractor MUST demonstrate SaaS compliance with applicable standards, and MAY do so through FedRAMP Authorization, CMS ATO/ATC, HITRUST r2 certification including the NY Security Regulatory Risk factor, a qualified third-party NIST control assessment, or another means approved by OHIP.	MUST	6.5 – SaaS
SEC-0080	The Contractor MUST provide OHIP with a client responsibility matrix (CRM) for the SaaS solution identifying where control responsibility is solely owned and where it is shared between the SaaS provider and its clients.	MUST	6.5 – SaaS
SEC-0081	All MES solutions containing MCD MUST establish 24/7 Security Operations Center capabilities for continuous monitoring, detection, and response.	MUST	7.1 – Continuous Security Ops
SEC-0082	All MES solutions MUST have a robust SIEM solution to collect, analyze, and correlate security-related logs and events.	MUST	7.2 – SIEM
SEC-0083	The Contractor MUST implement comprehensive frameworks and processes to comply with all federal certification requirements (ATO, ATC, IRS SCC, SSA TSSR).	MUST	8.1 – Framework and Processes
SEC-0084	The Contractor MUST maintain ongoing compliance with applicable State and federal regulations. This framework MUST address both initial certification and ongoing compliance.	MUST	8.1 – Framework and Processes
SEC-0085	The framework MUST include systematic processes for evaluating certification requirements and planning implementation approaches.	MUST	8.1 – Framework and Processes
SEC-0086	The Contractor MUST provide comprehensive support for achieving and maintaining CMS, IRS, and SSA audit, compliance, and certification requirements.	MUST	8.2 – Certification Support

SEC-0087	The Contractor SHOULD develop and maintain detailed certification tracking mechanisms that monitor progress toward certification milestones and provide clear visibility into certification status.	SHOULD	8.2 – Certification Support
SEC-0088	The Contractor MUST perform an inventory identifying all critical information system assets including hardware, software, firmware, data, applications, and communications equipment.	MUST	8.3 – Asset Management
SEC-0089	The Contractor SHOULD provide at minimum an annual System Component Inventory listing all managed and supported hardware and software licenses. The Department reserves the right to request the current inventory at any time.	SHOULD	8.3 – Asset Management
SEC-0090	The Contractor MUST establish comprehensive processes for supporting internal and independent third-party security audits.	MUST	8.4 – Audit Support
SEC-0091	The Contractor MUST maintain detailed tracking of all audit activities, findings, remediation plans, and verification of corrective actions.	MUST	8.4 – Audit Support
SEC-0092	The Contractor MUST perform routine vulnerability scans against the system or system components to identify vulnerabilities.	MUST	8.5 – Vulnerability Scanning
SEC-0093	The Contractor MUST provide access to SAST, DAST, and findings reports. The Department reserves the right to perform independent testing.	MUST	8.6 – Application Security Testing
SEC-0094	The Contractor SHOULD allow previews of actual Penetration Test Plan and Findings Reports prior to final submission. The Contractor MUST deliver all final Penetration Test Plans and Findings Reports to OHIP	SHOULD	8.7 – Penetration Testing
SEC-0095	The Contractor MUST tightly integrate their Incident Management process with existing OHIP incident management procedures.	MUST	8.8 – Incident Management
SEC-0096	All security and privacy events MUST be reported to the OHIP Security and Privacy Team in a timely manner.	MUST	8.8 – Incident Management
SEC-0097	The Contractor MUST promptly investigate and report determinations regarding any alleged or actual unauthorized use or disclosure of OHIP data.	MUST	8.8 – Incident Management
SEC-0098	The Contractor MUST submit a Corrective Action Plan with steps to prevent future unauthorized uses or disclosures.	MUST	8.8 – Incident Management

Appendix C: Legal and Regulatory Compliance

Bidders/Contractors **SHOULD** familiarize themselves with all applicable New York State and federal laws, regulations, policies, and standards for IT systems that transfer, process, or store Department data.

Finally, systems addressed by this Standard may be subject to security and regulatory requirements including, but not limited to:

- All applicable State and federal laws and regulations related to privacy protections
- New York State ITS policies and standards
- The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule
- Federal Trade Commission Health Breach Notification Rule
- New York Social Services Law (§) 367-b(4)
- New York State Social Services Law Section 369(4)
- New York State Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)
- Article 27-F of the New York Public Health Law (HIV/AIDS)
- 18 NYCRR 360-8.1
- NY Civil Rights 79-L
- Social Security Act, 42 USC 1396a(a)(7)
- Federal regulations at 42 CFR 431.302 and 42 CFR Part 2 (Substance Use Disorder)
- NYS Mental Hygiene Law Section 33.13
- 45 CFR Parts 160 and 164 (Privacy related sections for HIPAA)

Appendix D: Acronyms

The following acronyms are used throughout the OHIP Security, Privacy, and Compliance Domain Document.

ACA: Affordable Care Act
AI: Artificial Intelligence
AIDS: Acquired Immunodeficiency Syndrome
API: Application Programming Interface
ARC-AMPE: Acceptable Risk Controls for ACA, Medicaid, and Partner Entities (CMS framework)
ARS: Acceptable Risk Safeguards (CMS)
ATC: Authority to Connect
ATO: Authority to Operate
BAA: Business Associate Agreement
BCDR: Business Continuity and Disaster Recovery
CAP: Corrective Action Plan
CFR: Code of Federal Regulations
CMP: Continuous Monitoring Plan
CMS: Centers for Medicare & Medicaid Services
COTS: Commercial Off-The-Shelf
CRM: Client Responsibility Matrix
CTO: Chief Technology Office
DAST: Dynamic Application Security Testing
DB: Database
DBA: Database Administrator
DLP: Data Loss Protection
DMZ: Demilitarized Zone
DOH: Department of Health (New York State)
DOS: Division of Operations and Systems (New York State)
DUA: Data Use Agreement
ESSO: Enterprise Single Sign-On
FedRAMP: Federal Risk and Authorization Management Program
FIPS: Federal Information Processing Standards
FISMA: Federal Information Security Management Act
FTI: Federal Tax Information
GUI: Graphical User Interface
HCS: Health Commerce System (New York State, Department of Health)
HIPAA: Health Insurance Portability and Accountability Act of 1996
HITRUST: Health Information Trust Alliance
HIV: Human Immunodeficiency Virus
HTTPS: Hypertext Transfer Protocol Secure

IAM: Identity and Access Management
IDS: Intrusion Detection System
IdP: Identity Provider
IETF: Internet Engineering Task Force
IP: Internet Protocol
IPS: Intrusion Prevention System
IRC: Internal Revenue Code
IRS: Internal Revenue Service
ISRA: Information Security Risk Assessment
IT: Information Technology
ITS: Office of Information Technology Services (New York State)
JEA: Just-Enough-Access
JIT: Just-in-Time
JSON: JavaScript Object Notation
JWT: JSON Web Token
LDSS: Local Departments of Social Services
LLM: Large Language Model
MCD: Medicaid Confidential Data
MES: Medicaid Enterprise System
MFA: Multi-Factor Authentication
MH: Mental Health
mTLS: Mutual Transport Layer Security
NIST: National Institute of Standards and Technology
NYCRR: New York Codes, Rules and Regulations
NYS: New York State
OAuth: Open Authorization
OHIP: Office of Health Insurance Programs (New York State)
ONC: Office of the National Coordinator for Health Information Technology (New York State)
OS: Operating System
OWASP: Open Web Application Security Project
PHI: Protected Health Information
PII: Personally Identifiable Information
POA&M: Plan of Action and Milestones
PPSI: Personal, Private, or Sensitive Information
QNL: Quarterly Names List
RBAC: Role-Based Access Control
RDBMS: Relational Database Management System
REST: Representational State Transfer
RFC: Request for Comments
SaaS: Software-as-a-Service
SAST: Static Application Security Testing
SDLC: Solution Development Life Cycle
SDR: Standards Deviation Request
SFTP: Secure File Transfer Protocol
SHIELD Act: Stop Hacks and Improve Electronic Data Security Act (New York State)

SIEM: Security Information and Event Management

SMC: Streamlined Modular Certification (CMS)

SOC: Security Operations Center

SP: Special Publication (e.g., NIST SP 800-53)

SSA: Social Security Administration

SSL: Secure Sockets Layer

SSO: Single Sign-On

SSPP: System Security and Privacy Plan

STS: Security Token Service

SUD: Substance Use Disorder

TSSR: Technical System Security Requirements

USC: United States Code

UX: User Experience

VPN: Virtual Private Network

ZTA: Zero Trust Architecture