Access and Delivery Checklist

Ref #	System Review Criteria	Source	Guidance	IS/IP Certification Requirement	Project Initiation Milestone Evidence
Technical Service Classification: Business Intelligence					
TA.BI.10	The system of interest collects and stores data needed to produce reports consistent with data collection plan to assess quality and appropriateness of care furnished to participants of the waiver program.	Section 1115 of the Social Security Act, Section 1915(b) Freedom of Choice (Managed Care) Waivers, and Section 1915(c) Home and Community-Based Services Waivers)	This applies to the Medicaid waiver program. Evidence could include waiver data collection plan (R1) along with technical designs for collecting relevant data and test reports (R2), and actual reports (R3). Enterprise: State needs to have a data collection plan that explains what data will be collected and how it will be used to improve quality of care. Needs to ensure all relevant data is being collected across data-generating modules. Module: This applies to modules that supports generation, storage and retrieval waiver program data, its processing and reporting. This criterion is not applicable to E&E.	No	EDW ITN B.3.F.5.c(1) SR-217 Table 34
TA.BI.2	The system of interest supports a range of analysis actions. (These include benefit modeling, utilization management, provider-member-MCO profiling, program planning, forecasting, program assessment, provider or contractor performance, quality assurance, fraud detection, comparison of fee-for-service and managed care, statistical analysis, comparative analysis, financial trends, case-mix adjustments within time ranges specified in the APD and/or RFP, and other functions as described in the APD and/or RFP.)	MMIS BP	This criterion may not apply to E&E. Evidence can include plans to acquire or develop a data analysis capability (R1), requirements documents and test scenarios/reports (R2), demonstration of the analysis capability (R3). State: RFPs or plans must include the functions listed in the criterion. This may involve more than one module as well as program management process. State must ensure that relevant modules are working seamlessly to produce the necessary analysis. Module: This applies to modules that support a broad spectrum of data analytics, system, user, and ad hoc query reporting, and to third-party product(s) if used to support this criterion.	No	EDW ITN B.3.F.5.c(1) SR-218 Table 34
TA.BI.4	The system of interest collects and summarizes data for specific user communities (e.g. data marts or cubes) such as program analysis staff, research group, financial management unit, agency executives (e.g. dashboard).	MMIS BP	Evidence could include plans to include this capability (R1), requirements documents and test scenarios/reports (R2), demonstration and actual reports (R3). State: The state has talked with stakeholders (for example fraud detection team or AG office) to understand their needs and has configured the system such that the stakeholders can get the data in the form they need it. Module: This applies to modules that gather, collect and process data, provide system, user, and ad hoc query reporting.	No	EDW ITN B.3.F.5.c(1) SR-219 Table 34

TA.BI.5	The system of interest provides reports that allow users to drill down from summarized data to detailed data.	IBP	Evidence includes plans to include this capability (R1), requirements documents and integration test reports (R2), demonstration (R3). State: If drill-down involves viewing data across modules, the state must ensure that this happens correctly across modules / sub-systems. Module: This applies to modules that provide user reporting and ad hoc query reporting.	No	EDW ITN B.3.F.5.c(1) SR-220 Table 34
TA.BI.7	The system of interest's business intelligence information is consistent and reliable with full automation.	IBP	Evidence could include plans to test the internal consistency and quality of the data and reports (R1), test reports (R2), and attestation (R3). Enterprise: The state regularly checks the quality of the data to ensure accurate and reliable results. Module: This applies to modules that maintain business intelligence information, and to third-party product(s) if used to support this criterion.	No	EDW ITN B.3.F.5.c(1) SR-221 Table 34
TA.BI.9	The system of interest limits access to authorized group of stakeholders.	MITA 3.0 TCM ML3	Evidence can include high-level requirements and role-based mapping (R1), role-based test reports (R2), and demonstration (R3). Enterprise: The system is capable of restricting access to individual screens and data according to role across all relevant modules. Module: This applies to modules that provide user interfaces or supply data to users.	Yes	B.4.D.5 Security IP.5.11 Figure 8 EDW ITN B.3.F.5.c(1) SR-222 Table 34
Technical Service Classification: Client Support					
TA.CS.10	The system of interest's user interface or associated interfaces provides text titles for frames to facilitate frame identification and navigation.	MITA 3.0 Part III, Ch. 7	Evidence can include plans to include these capabilities (R1) and screenshots (R2, R3). Modules: This applies to modules that have user interfaces.	Yes	B.4.D.5 Security B.4.D.6 Master Data Management EDW ITN B.3.F.5.c(1) SR-223 Table 34

TA.CS.14	The system of interest provides member and provider access to services via browser, kiosk, voice response solution, or mobile device, and manual submissions.	MITA 3.0 TCM ML2	Evidence can include high-level requirements and RFP language showing intent to develop these capabilities (R1), test reports and demonstration (R2, R3). Enterprise: The state ensures that these services and processes work seamlessly across all relevant modules. Module: Modules with user interfaces integrate with the state's solution for providing access to users via various means.	NA	Recipient and Provider Modules
TA.CS.17	The system of interest conforms to usability and design standards set by the state. This includes aesthetics, consistency in the user interface, and visual quality of the interfaces.	MITA 3.0 Ch. 4 (usability)	Evidence can include high-level requirements and RFP language showing intent to implement design standards (R1) and screenshots (R2, R3). Enterprise: The state ensures that aesthetics are consistent across the modules. Module: The user interface screens should be configurable so that they can be made to fit the state's user interface design criteria.	Yes	B13. Compliance EDW ITN B.3.F.5.c(1) SR-224 Table 34
TA.CS.18	The system of interest fully complies with section 508 accessibility.	MITA 3.0 Ch. 4 Fig. 4-3 (508 compliance)	Evidence can include high-level requirements and RFP language showing intent to develop these capabilities (R1), and 508 compliance test reports (R2, R3). Enterprise: The state should ensure that all internal and external users can access any relevant module and / or screen with assistive technology. Module: This applies to modules that provide system-to-system and user interfaces.	Yes	B13. Compliance Figure 33 EDW ITN B.3.F.5.c(1) SR-225 Table 34
TA.CS.6	To the greatest extent possible, the system of interest is browser agnostic.	IBP	Evidence can include RFPs requiring contractors to develop and test compatibility with various browsers (R1), test reports and demonstrations (R2,R3). Enterprise: The state should ensure that the modules and overall system are compatible with the most popular browsers. Some examples include Safari, Good Chrome, Mozilla Firefox and Microsoft Internet Explorer. Module: Modules with user-facing screens must work with popular browsers.	Yes	B13. Compliance Figure 33 EDW ITN B.3.F.5.c(1) SR-226 Table 34
Technical Service Classification: Forms and Reporting					
TA.FR.1	The system of interest supports retrieval and presentation of data associated with geographic indicators such as state, county, and zip code.	IBP	Evidence can include data plans to include these capabilities (R1), showing which data is associated with geographic indicators (such as in state data models) (R2), demonstration of retrieval by geographic indicators (R3). Enterprise: The state ensures that data can be associated with geographic indicators across all relevant modules. Module: This applies to modules that edit, store, retrieve, present, and/or report data that have geographic indicators associated with them.	No	EDW ITN B.3.F.5.c(1) SR-227 Table 34

TA.FR.2	The system of interest supports federal reporting requirements when these requirements are met through the decision support services (DSS).	SMM	Evidence can include plans to include ability to generate and send all mandatory federal reports (R1), test reports (R2), and actual reports (R3). Enterprise: The state ensures that all modules works seamlessly to generate the reports. Module: Modules should show how they are contributing relevant data (if applicable) through interoperability standards adopted by the state.	No	EDW ITN B.3.F.5.c(1) SR-228 Table 34
TA.FR.4	The system of interest supports a variety of formats and output options (e.g. Word, Excel, html, Access database, or GUI formats).	SMM	Evidence can include plans to include this requirement (R1), test scenarios/reports or copies of the sample report in various formats (R2, R3). Module: This criterion applies to modules with a data export function.	Yes	B.4.B.3 System Documentation EDW ITN B.3.F.5.c(1) SR-229 Table 34
TA.FR.6	The system of interest supports simple queries and pre-formatted reports that are easy to access, follow a user-friendly protocol, and produce responses immediately.	SMM	Pre-formatted reports should not take an inordinate amount of time to run, meaning that sufficient capacity must be built into the system. Queries should be easy to use. Evidence can include plans to design frequently run reports, along with enough computing power to return responses for them immediately without slowing other system functions (R1), test scenarios/reports and demonstrations (R2, R3). Module: This applies to modules providing simple ad hoc data query support, and selection by users of predetermined / preformatted reports.	Yes	B.6 Reporting Requirements EDW ITN B.3.F.5.c(1) SR-230 Table 34
TA.FR.7	The system of interest provides ad hoc reporting capability that presents summarized information on key factors (e.g. number of enrollees, total dollars paid) to executive staff upon request.	SMM	Evidence can include plans to include this capability (R1), test reports (R2), and demonstration (R3). The state ensures that all modules works seamlessly to generate the reports. Module: This applies to modules that provide ad hoc reporting capability and user interfaces.	No	EDW ITN B.3.F.5.c(1) SR-231 Table 34
TA.FR.8	The system of interest provides ad hoc query capability for retrieval of data relevant to specific operational units, e.g. claims resolution, prior authorization, and medical necessity review.	SMM	Evidence can include plans to include this capability (R1), test reports (R2), and demonstration (R3). The state ensures that all modules works seamlessly to generate the reports. Module: This applies to modules that provide ad hoc query capability and user interfaces.	No	EDW ITN B.3.F.5.c(1) SR-232 Table 34

TA.FR.9	The system of interest produces report for each primary care case manager (PCCM) identifying the PCCM’s enrollees and the total payment per month per enrollee.	IBP	This criterion is not applicable to E&E. Evidence can include plans to include this capability (R1), test reports (R2), and demonstration (R3). The state ensures that all modules works seamlessly to generate the reports. Module: This applies to modules that provide reporting capability for PCCM stakeholder.	No	PCCM is no longer being used by the Agency.
Technical Service Classification: Performance Measurement					
TA.PM.5	The system of interest's transactions execute in a reasonable amount of time.	MITA 3.0 TCM ML3	This criterion speaks to the need to conduct good capacity management practices. The state and its contractors should anticipate capacity needs and design and manage to meet current and future needs. Evidence can include plans to perform capacity management processes (R1), and performance testing and capacity monitoring reports (R2, R3). Enterprise: The state has defined acceptable transaction times for various transaction types, understands and documents which modules are involved in which transactions, defines performance requirements and determines capacity needs against those requirements, acquires necessary capacity, monitors system performance, and periodically	Yes	B.4.D.14 Performance Standards Figure 17 EDW ITN B.3.F.5.c(1) SR-233 Table 34
TA.PM.6	The system of interest collects information in predefined formats.	MITA 3.0 TCM ML2	Evidence could be plans to include this capability (R1), requirements documents and test scenarios/reports (R2), demonstration (R3). Enterprise: The state has defined formats with which to collect information across the modules. Module: Modules that collect information adhere to the state's predefined formats.	Yes	B.4.D.1 Integration Platform IP.1.15 Figure 4 EDW ITN B.3.F.5.c(1) SR-234 Table 34

TA.PM.7	The system of interest provides the ability to record and monitor the performance and utilization of resources within the overall system.	MITA 3.0 Ch. 4 (business transaction management)	Evidence can include plans to include this capability (R1), monitoring reports (R2, R3). Enterprise: The state is able to monitor/review and assess performance and resources utilization across the modules. Module: The module is capable of monitoring and reporting the performance and utilization of resources, if applicable.	Yes	B.4.D.3 Managed File Transfer IP.3.3 B.4.D.7 Integration IP.7.24 EDW ITN B.3.F.5.c(1) SR-235 Table 34
TA.PM.8	The system of interest generates performance measures for specific business processes using predefined and ad hoc reporting methods.	MITA 3.0 TCM ML2	Evidence can be plans to include this capability (R1), requirements documents and test scenarios/reports (R2), demonstration (R3). Enterprise: The state has defined the performance measures it intends to measure for specific business processes. Module: This applies to modules that generate performance measures for specific business processes based on state predefined performance measures.	Yes	B.4.D.3 Managed File Transfer B.4.D.7 Integration EDW ITN B.3.F.5.c(1) SR-236 Table 34
Technical Service Classification: Security and Privacy					
TA.SP.10	The system of interest must protect electronic protected health information (ePHI) from improper alteration or destruction including authentication mechanisms and to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	45CFR164.310	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence can include plans to include this capability (R1), test reports (R2), and demonstration (R3) documented in the System Security Plan (SSP) to ensure the confidentiality, integrity, and availability of the data, as well as ongoing risk assessment to ensure its compliance. Enterprise: The ongoing risk assessment needs to cover all operating modules. Module: This criterion may be applicable to modules that provide this functionality.	Yes	B.4.D.5 Security IP.5.35 Figure 8 EDW ITN B.3.F.5.c(1) SR-237 Table 34

TA.SP.11	The system of interest must verify that a person or entity seeking access to electronic protected health information is the one claimed.	45CFR164.310	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence can include plans to include this capability (R1), test reports (R2), and demonstration (R3) documented in the System Security Plan (SSP) to ensure the confidentiality, integrity, and availability of the data, as well as ongoing risk assessment to ensure its compliance. Enterprise: The ongoing risk assessment needs to cover all operating modules. Module: This criterion may be applicable to modules that provide this functionality	Yes	B.4.D.5 Security IP.5.2 Figure 8 EDW ITN B.3.F.5.c(1) SR-238 Table 34
TA.SP.13	The agency must publish provisions governing the confidential nature of information about applicants and beneficiaries including the legal sanctions imposed for improper disclosure and use.	42CFR431.304	Evidence should include the state public notice provisions on system of interest website and/or written form. Evidence can include plans to include this capability (R1), screen shot and/or paper form artifact (R2 and R3). Module: This criterion may be applicable to modules that provide this	NA	Agency Policy (PHI and PII) - HIPAA and HITECH
TA.SP.14	The Medicaid Agency must demonstrate how the System of Interest publicize copies of the provisions governing the confidential nature of information about applicants and beneficiaries, including the legal sanctions, in addition provide copies of the provision to applicants, beneficiaries and other persons and agencies to whom information is disclosed	42CFR431.304	Evidence should include the state's standard operating procedure on publishing, updating, and changing public notice provisions governing the confidential nature of PII/PHI collected, used, processed, and disclosed for the system of interest. Evidence can include plans to include this capability (R1), SOP document, screen shot, and demonstration (R2 and R3). Module: This criterion may be applicable to modules that provide this functionality	NA	On Agency Portals for external users. Providers are covered entities.

TA.SP.15	The Medicaid Agency must demonstrate how the system of interest follows regulations govern the safeguard of information about applicants and beneficiaries. The following is the minimal set of information that must be safeguarded (1) Names and addresses; (2) Medical services provided; (3) Social and economic conditions or circumstances; (4) Agency evaluation of personal information; (5) Medical data, including diagnosis and past history of disease or disability; and (6) Any information received for verifying income eligibility and amount of medical assistance payments. Income information received from SSA or the Internal Revenue Service must be safeguarded according to the requirements of the agency that furnished the data. (7) Any information received in connection with the identification of legally liable third party resources.	42CFR431.305	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist and because of ePHI classification. Evidence should include system of interest's System Security Plan (SSP) regarding the technical, operational, and administrative safeguard procedures and compensating controls of applicants PII and PHI according the HIPAA Security Rule (R1, R2, R3). Enterprise: The state should document the safeguarding policies and procedures and compensating controls of applicants' and beneficiaries' PII and PHI at the SMA enterprise level. Module: This criterion may be applicable to modules that provide this functionality.	Yes	B.4.D.5 Security IP.5.1 Figure 8 EDW ITN B.3.F.5.c(1) SR-239 Table 34
TA.SP.18	The system of interest complies with provisions for Administrative Simplification under the HIPAA of 1996 to ensure the confidentiality, integrity, and availability of ePHI in transit and at rest: • Provides safeguards as described in the October 22, 1998 State Medicaid Director letter, Collaborations for Data Sharing between State Medicaid and Health Agencies; • Performs regular audits; and • Supports incident reporting.	HIPAA	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include 1) showing use of the policies, procedures, and compensating technical, administrative, and operational controls, 2) document incident/breach notification procedures and process, 3) demonstrating the use of encryption for protection of PHI/PII in transit and at rest, and 4) performing regular risk assessment or audit on the system of interest. Enterprise: The state should document the safeguarding policies and procedures and compensating controls of applicants' and beneficiaries' PII and PHI at the SMA enterprise level. Module: This criterion may be applicable to modules that provide this functionality.	Yes	B.4.D.5 Security IP.5.35 Figure 8 EDW ITN B.3.F.5.c(1) SR-240 Table 34

TA.SP.22	The system of interest verifies identity of all users, denies access to invalid users. For example: • Requires unique sign-on (ID and password) • Requires authentication of the receiving entity prior to a system initiated session, such as transmitting responses to eligibility inquiries.	45 CFR 164.308(a) (4) (i) 45 CFR 164.312(a) (2) (i) 45 CFR 164.312(d)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include documentation of accounts management in SSP (R1, R2), and test reports and demonstrations (R2, R3). Enterprise: The state should be able to demonstrate this capability for all modules. Module: Module should show that it complies with user authentication and authorization controls.	Yes	B.4.D.5 Security IP.5.16 Figure 8 EDW ITN B.3.F.5.c(1) SR-241
TA.SP.23	The system of interest supports data integrity through system controls for software program changes and promotion to production.	IBP	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include documented configuration and change management plans and controls in the system of interest SSP (R1, R2, R3). Enterprise: The state should have policies and procedures in place that apply across modules. Modules: Module configuration or code changes are controlled through configuration and change management processes and adhere to the SPP.	Yes	B.4.D.9 Implementation and Acceptance Figure 12 EDW ITN B.3.F.5.c(1) SR-242 Table 34
TA.SP.24	The system of interest enforces password policies for length, character requirements, and updates.	45 CFR 16.308(a) (5) (i) (D)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include policies documented in the technical controls section of the SSP (R1, R2), demonstrations and regular continuous monitoring and risk assessment (R3). Enterprise: The state should have password policies that apply across all modules. Modules: This applies to modules that require or validate passwords.	Yes	B.4.D.5 Security Figure 8 EDW ITN B.3.F.5.c(1) SR-243 Table 34
TA.SP.25	The system of interest supports a user security profile that controls user access rights to data categories and system functions.	45 CFR 164.308(a) (ii) (B) 45 CFR 164.308(a) (3) (i) 45 CFR 164.310(a) (2) (iii)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include documentation in the technical controls section of the SSP (R1, R2, R3) and test reports and demonstrations (R2, R3). Enterprise: The state should ensure consistent and enforceable security profiles and access rights to various data categorizations that apply across the modules in the enterprise. Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security Figure 8 EDW ITN B.3.F.5.c(1) SR-244 Table 34
TA.SP.26	The system of interest permits supervisors or other designated officials to set and modify user security access profile.	45 CFR 164.308(a) (3) (ii) (A)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include Role Based Access Control (RBAC) according to the system of interest; SSP technical controls during design/implementation phase (R1,R2); demonstrations and screenshots (R3). Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security IP.5.15 Figure 8 EDW ITN B.3.F.5.c(1)

TA.SP.27	The system of interest includes procedures for accessing necessary electronic Protected Health Information (ePHI) in the event of an emergency; continue protection of ePHI during emergency operations.	45 CFR 164.312(a) (2) (ii) 45 CFR 164.308(a) (7) (ii) (C)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include Business Continuity, Disaster Recovery, and Incident Management Plans (R1, R2,R3). Enterprise: The plans should cover every module. Module: The module needs to be included in the plans mentioned above.	Yes	B.4.D.13 Disaster Recovery IP.13.2 EDW ITN B.3.F.5.c(1) SR-246 Table 34
TA.SP.28	The system of interest supports workforce security awareness through such methods as security reminders (at log on or screen access), training reminders, online training capabilities, and/or training tracking.	45 CFR 164.308(5) (i)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include training documentation in the administrative controls section of SSP (R1, R2, R3). Enterprise: The state should ensure that all modules are covered by the regular and relevant security and privacy awareness training. Modules: This applies to modules that support this security and privacy awareness training and tracking functionality	Yes	B.4.D.10 Training Figure 13 B.4.E.6 Figure 22

TA.SP.3	The system of interest supports SMA in its responsibility for (i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations. (ii) Implementation specifications: (A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). (C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. (D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	45CFR164.308	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include SMA policies, procedures, plans, implementation of HIPAA and NIST-based technical, administrative, and operational controls in terms of risk analysis, risk management and mitigation, sanction policy, and continuous monitoring and oversight (R1, R2); demonstrations and ongoing regular risk assessment and analysis report regarding the effectiveness of its implementation (R3).	Yes	B.10.4 Deliverables PP-5 System Security Plan EDW ITN B.3.F.5.c(1) SR-247 Table 34
TA.SP.30	The system of interest alerts appropriate staff authorities of potential violations of privacy safeguards, such as inappropriate access to confidential information.	45 CFR 164.308(a) (6) (i) 45CFR 164.308(a) (6) (ii)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include access violation notification and altering, data leak prevention, and incident/breach notification and escalation process and procedure documented in SSP (R1, R2, R3) and test reports of the functionality (R2); demonstrations and sample artifacts of incident/breach notification (R3). Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security IP.5.17 Figure 8 EDW ITN B.3.F.5.c(1) SR-248 Table 34

TA.SP.31	The system of interest provides right of access and request for access to individuals to protect PHI in a timely manner that allows it to be included in responses to inquiries and report requests.	45 CFR 164.524(b) (1) 45 CFR 164.524(a) (1)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include the system of interest addresses applicants and beneficiaries right of access, reporting, and inquiries to their PHI/PII data. Modules: This applies to modules that support this functionality	No	EDW ITN B.3.F.5.c(1) SR-251 Table 34
TA.SP.32	The system of interest contains verification mechanisms that are capable of authenticating authority (as well as identify) for the use or disclosure requested. For example: • Denies general practitioner inquiry for recipient eligibility for mental health services • Permits inquiries on claim status only for claims submitted by the inquiring provider.	45 CFR 164.312(a) (1).	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist and because of ePHI classification. Evidence should include authentication and authorization guidelines based on roles and responsibilities and align with relevant HIPAA security and privacy rules as documented in the system of interest's SSP (R1, R2, R3) and test reports and demonstration of the functionality (R2, R3). Enterprise: The state ensures that this applies across all relevant modules within the enterprise. Modules: This applies to modules that support this functionality	Yes	IS/IP ITN B.4.D.5 IP.5.2 Figure 8 EDW ITN B.3.F.5.c(1) SR-250 Table 34
TA.SP.33	The system of interest supports encryption and decryption of stored ePHI or an equivalent alternative protection mechanism.	45 CFR 164.312(a) (2) (iv)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include technical controls documented in the system of interest's SSP (R1, R2, R3) and demonstration of the encryption (R2, R3). Enterprise: The state needs to make sure that this is applied across relevant modules. Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 -Security IP.5.3 Figure 8 EDW ITN B.3.F.5.c(1) SR-251 Table 34
TA.SP.34	The system of interest supports encryption of ePHI that is being transmitted, as appropriate.	45 CFR 164.312(e) (2) (ii)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include technical controls documentation, implementation, and demonstration as described in SSP (R1, R2, R3). Enterprise: The state needs to make sure that this is applied across relevant modules. Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 -Security IP.5.3 Figure 8 EDW ITN B.3.F.5.c(1) SR-252 Table 34

TA.SP.35	The system of interest supports integrity controls to guarantee that transmitted ePHI is not improperly modified without detection (e.g. provide secure claims transmission).	45 CFR 164.312(e) (1)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include technical controls design, implementation, and demonstration as described in SSP (R1, R2, R3). Enterprise: The state needs to make sure that this is applied across relevant modules. Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security IP.5.3 Figure 8 EDW ITN B.3.F.5.c(1) SR-253 Table 34
TA.SP.36	The system of interest provides data integrity of ePHI by preventing and detecting improper alteration or destruction (e.g. double keying, message authentication, digital signature, check sums etc).	45 CFR 164.312(c) (1) 45 CFR 164.312(d) (2) (i)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include technical safeguard countermeasures regarding ePHI data integrity controls in design, implementation, and demonstration as described in SSP (R1, R2, R3). Enterprise: The state needs to make sure that this is applied across relevant modules. Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security IP.5.3 Figure 8
TA.SP.37	The system of interest provides the capability that all system activity can be traced to a specific user or entity.	IBP	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include audit controls as documented in SSP (R1, R2, R3) and test reports and demonstrations (R2, R3). Enterprise: User activities should be traced across all modules. Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security IP.5.6 Figure 8 EDW ITN B.3.F.5.c(1) SR-254 Table 34
TA.SP.38	The system of interest identifies and responds to suspected or known security and privacy incidents; mitigate, to the extent practicable, harmful effects of security and privacy incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. (Such as logon attempts that exceed maximum allowed.)	45 CFR 164.308(a) (6) (ii) 45 CFR 164.312(a) (2) (iii)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include incident handling guide based on NIST SP 800-61 (R1, R2, R3), and test reports and demonstrations (R2, R3). Enterprise: The state ensures that monitoring, alerting, containment, eradication, and recovery are being generated across all modules. Modules: This applies to modules that support this functionality.	Yes	B.4.D.11 Hosting and Environment IP.11.18 Figure 14 EDW ITN B.3.F.5.c(1) SR-255 Table 34

TA.SP.39	The system of interest logs system activity and enables analysts to examine system activity in accordance with audit policies and procedures (error diagnosis, and performance management) adopted by the Medicaid agency.	45 CFR 164.312(b)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include audit controls (logging and examine) under technical, operational, and management controls in SSP (R1, R2, R3) and actual system logs and audit reports (R2, R3). Enterprise: The state ensures that logs and audits cover all relevant modules. Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security IP.5.3 Figure 8 EDW ITN B.3.F.5.c(1) SR-256 Table 34
TA.SP.41	The system supports procedures for guarding, monitoring, and detecting malicious software (e.g. viruses, worms, malicious code, etc.).	45 CFR 164.308(a) (5) (ii) (B)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include the implementation of intrusion detection system (IDS) and intrusion prevention system (IPS) monitoring in technical controls in SSP (R1, R2, R3); regular ongoing IDS/IPS report and continuous monitoring activities (R3). Modules: This applies to modules that support this functionality.	Yes	B.4.D.11 Hosting and Environment IP.11.15 Figure 14 EDW ITN B.3.F.5.c(1) SR-257 Table 34
TA.SP.42	The system of interest has the capability to provide provision of access to an authorized user or request.	45 CFR 164.524(c)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include user account provisioning and authorization documented in SSP (R1, R2) and demonstration (R2, R3). Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security IP.5.16 Figure 8 EDW ITN B.3.F.5.c(1) SR-258 Table 34
TA.SP.43	The system of interest contains indicators that can be set to restrict distribution of ePHI in situations where it would normally be distributed.	45 CFR 164.502 (C) 45 CFR 164.522(a) (1) (iii)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include the system of interest's capability of restricting uses or disclosures of ePHI about the individual to carry out treatment, payment, or healthcare operations (R1, R2) and demonstration (R2, R3). Modules: This applies to modules that support this functionality.	Yes	B.4.D.5 Security IP.5.35 Figure 8 EDW ITN B.3.F.5.c(1) SR-259 Table 34

TA.SP.44	The system tracks disclosures of ePHI; provides authorized users access to and reports on the disclosures.	45 CFR 164.528(a) (3) 45 CFR 164.528(b)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should be the system of interest's capability of handling individual request of receiving an accounting of disclosures of ePHI made by a covered entity in the six years prior to the date on which the accounting is requested (R1, R2), and demonstration (R3). Further guidance can be found in 45 CFR 164.528(c) and 45 CFR 164.528(d). Modules: This applies to modules that support this functionality.	No	EDW ITN B.3.F.5.c(1) SR-260 Table 34
TA.SP.45	The system of interest has the capability to handle request for amendment and timely action of making amendments ePHI about the individual in a designated record set	45 CFR 164.526(a) (1) 45 CFR 164.526(b) (1) and 45 CFR 164.526(c) (1)	For E&E only, the state need not supply evidence for this criterion because of ePHI classification. Evidence should include the system of interest's capability of handling an individual request for amendment ePHI and making amendments in a timely fashion according to 45 CFR 164.526 CFR (R1, R2), and demonstration (R3). Modules: This applies to modules that support this functionality.	No	EDW ITN B.3.F.5.c(1) SR-261 Table 34
TA.SP.46	The SMA has a Contingency Plan (CP) for the system of interest that: identifies essential missions and business functions and associated contingency requirements. These requirements include recovery objectives, restoration priorities, contingency roles, responsibilities and addresses maintaining essential business functions despite an information system disruption, compromise, or failure. This plan should be reviewed and updated on a yearly basis.	45CFR164.208(7)(i) and 45CFR164.208(7)(ii)	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include contingency / continuity of operations and disaster recovery plans (R1, R2, R3) and evidence of exercises or scheduled exercises to test them (R2, R3). Enterprise: The state ensures that all modules are covered under the contingency / continuity of operations and disaster recovery plans and that the plans are updated and tested regularly. Module: The module is covered under the plans and testing exercises.	Yes	B.4.E.8 Disaster Recovery and Business Continuity Figure 24 EDW ITN B.3.F.5.c(1) SR-262 Table 34
TA.SP.48	An alternate storage site should be identified, including necessary agreements to permit the storage and recovery of system backup information and the resumption of system operations for business functions within the time period specified. The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential business functions.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include contingency / continuity of operations and disaster recovery plans (R1, R2, R3) and evidence of exercises or scheduled exercises to test them (R2, R3). Enterprise: The state ensures that all modules are covered under the contingency / continuity of operations and disaster recovery plans and that the plans are updated and tested. Module: The module is covered under the plans, alternate storage facility, and testing exercises.	Yes	B.4.E.8 Disaster Recovery and Business Continuity Figure 24 EDW ITN B.3.F.5.c(1) SR-262 Table 34

TA.SP.49	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include contingency / continuity of operations and disaster recovery plans (R1, R2, R3) and evidence of exercises or scheduled exercises to test them (R2, R3). Enterprise: The state ensures that all modules are covered under the contingency / continuity of operations and disaster recovery plans and that the plans are updated and tested. Module: The module is covered under the plans, recovery, and testing exercises.	Yes	B.4.D.13 Disaster Recovery and Business Continuity EDW ITN B.3.F.5.c(1) SR-264 Table 34
TA.SP.5	The system must have standard Access Control specifications to include: (i) Assigning a unique name and/or number for identifying and tracking user identity. (Required) (ii) Establishing and implementing as needed emergency access procedures for obtaining necessary electronic protected health information during an emergency. (Required). (iii) Implementing electronic procedures that terminate an electronic session after a predetermined time of inactivity. (Addressable) (iv) Implementing a mechanism to encrypt and decrypt electronic protected health information. (Addressable)	45CFR164.310	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist and because of ePHI classification. Evidence should include documented access controls specifications in SSP (R1, R2) and test reports and demonstrations (R2, R3). Enterprise: the state ensures that all modules are covered under the same consistent and reasonable SMA access control specifications. Module: This is applicable to modules and must adhere to the same consistent access controls specifications and standards.	Yes	B.4.D.5 Security IP.5.2 Figure 8 EDW ITN B.3.F.5.c(1) SR-265 Table 34
TA.SP.50	Roles and responsibilities of individuals should be separated through assigned information access authorization as necessary to prevent malevolent activity.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include role based access control policy in SSP (R1, R2) and test reports and demonstrations (R2, R3). Enterprise: the state ensures that all modules are covered under the same consistent and reasonable SMA access control specifications. Module: This is applicable to modules and must adhere to the same consistent access controls specifications and standards.	Yes	B.4.D.5 Security IP.5.2 Figure 8 EDW ITN B.3.F.5.c(1) SR-266 Table 34

TA.SP.51	User account access authorization should follow the concept of least privilege; allowing users access to only the information that is necessary to accomplish assigned tasks in accordance with business functions.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include role based access controls policy in SSP (R1, R2), demonstration of its use and ongoing effectiveness through continuous monitoring (R3). Enterprise: The state ensures that all modules are covered under the same consistent role based access control specifications and policy. Module: The module is covered under the specifications.	Yes	B.4.D.5 Security IP.5.29 Figure 8 EDW ITN B.3.F.5.c(1) SR-267 Table 34
TA.SP.52	Accounts should be disabled after 3 consecutive invalid login attempts.	IBP	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include this policy documented in technical controls, control AC-7 in SSP (R1, R2, R3). Enterprise: The state ensures that all modules are covered under the same consistent specification. Module: The module is covered under the specification.	Yes	B.4.D.5 Security IP.5.31 Figure 8
TA.SP.53	User account access should be reviewed on a quarterly basis at a minimum. User accounts should be appropriately disabled as roles and responsibilities change.	IBP	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include this policy documented in account management (AC-2) policy in SSP (R1, R2, R3), and evidence that the user accounts are reviewed at least quarterly. Enterprise: The state ensures that all modules are covered under the policy and that the reviews are happening quarterly	Yes	B.4.D.5 Security IP.5.15 Figure 8 Deliverable PP-5 System Security Plan
TA.SP.54	After 15 minutes of inactivity, the system should initiate a session lock; the session lock should remain in place until the user reestablishes access using established identification and authentication procedures.	IBP	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include this policy in technical controls, control AC-7 in SSP (R1, R2, R3), and demonstration (R2, R3). Enterprise: The state should ensure that this is applied to all modules.	Yes	B.4.D.5 Security IP.5.37 Figure 8 EDW ITN B.3.F.5.c(1) SR-268 Table 34

TA.SP.55	The system of interest supports or regulates connections with other information systems (e.g. system of interest to outside of the SMA authorization boundary) through the use of Interconnection Security Agreements. Interconnection Security Agreements document, the interface characteristics, security requirements, and the nature of the information communicated over the connection.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include this policy documented in Interconnection Security Agreements or MOU or data sharing agreements (R1, R2, R3). Enterprise: The consistent application of reasonable and appropriate security, privacy, and business agreements to ensure the safeguard of transmission and exchange of ePHI/PII.	Yes	B.4.D.5 Security IP.5.20 Figure 8
TA.SP.56	The SMA enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible).	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include this policy documented in the physical and environmental protection (PE-2) section of SSP. Enterprise: The state must confirm that all contractor facilities that host the Medicaid systems are secure according to state policies. State should provide audit reports to that effect.	Yes	B.4.D.11 Hosting and Environment IP.11.20 Figure 14 EDW ITN B.3.F.5.c(1) SR-269 Table 34
TA.SP.57	The SMA maintains a current list of personnel with authorized access to the space where required (e.g. review and approval of access list and authorization credentials at least once every 180 days, removes personnel from the access list that no longer require access).	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include this policy documented in Physical and Environmental Protection (PE-3) section of SSP (R1, R2, R3) and a copy or demonstration of the most recent list (R2, R3). Enterprise: The state must ensure that this list is being maintained and monitored.	Yes	B.4.D.5 Security IP.5.25 Figure 8 EDW ITN B.3.F.5.c(1) SR-270 Table 34
TA.SP.58	Physical access to information system distribution and transmission lines is controlled within the facility to prevent unauthorized access.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include this policy documented in the Physical and Environmental Protection (PE-4) section of SSP. Enterprise: The state must confirm that all contractor facilities that host the Medicaid systems comply with this control. State should provide audit reports to that effect.	Yes	B.4.D.11 Hosting and Environment IP.11.20 Figure 14 EDW ITN B.3.F.5.c(1) SR-271 Table 34

TA.SP.6	The system must guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	45CFR164.310	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include the countermeasures and proper safeguard implementation of technical, operational, and administrative security and privacy controls documented in the SSP (R1, R2), demonstration, audit report, and ongoing risk assessment and analysis (R3). Enterprise: The state must confirm that all business partners and downstream entities comply with this control. State should provide audit reports to that effect.	Yes	B.4.D.5 Security IP.5.16 Figure 8 EDW ITN B.3.F.5.c(1) SR-272 Table 34
TA.SP.61	A short-term uninterruptible power supply should be employed to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include policy documented in Physical and Environmental Protection (PE-11) section of SSP (R1, R2, R3). Enterprise: The state must confirm that all contractor facilities that host the Medicaid systems comply with this control. State should provide audit reports to that effect.	Yes	B.4.D.13 Disaster Recovery and Business Continuity EDW ITN B.3.F.5.c(1) SR-273 Table 34
TA.SP.63	The system of interest provides staff with Single Sign-On (SSO) functionality to a majority of the applications in the State Medicaid Enterprise.	MITA 3.0 TCM ML3	Evidence could be plans to include single-sign-on capabilities (R1), test reports and demonstrations (R2,R3). Enterprise: State ensures this is met across all modules. Module: Module supports single sign-on.	Yes	B.4.D.5 Security Figure 8
TA.SP.7	The SMA implements policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information.	45CFR164.310	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist and because of ePHI classification. Evidence should include the Media Protection (MP) section of the SSP (R1, R2, R3). Enterprise: The state has policies and procedures for protecting ePHI when transferring and disposing of equipment. The state ensures that its contractors are following the procedures. State should provide audit reports to that effect.	Yes	B.4.D.5 Security IP.5.36 Figure 8 EDW ITN B.3.F.5.c(1) SR-274 Table 34

TA.SP.70	The system of interest enforces a sufficient level of authentication / identification against fraudulent transmission and imitative communications deceptions by validating the transmission, message, station or individual.	IBP	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include the relevant identification, authentication, system, and information integrity technical controls section of the SSP (R1, R2); demonstration, audit, and ongoing security risk assessment and analysis (R3). Enterprise: The state must ensure that its business partners and downstream entities are complying with the state's policies in a consistent and effective manner. State should provide audit reports to that effect. Module: This applies to modules that process, store, manage, disclose, and use ePHI/PII.	yes	B.4.D.5 Security IP.5.3 Figure 8 EDW ITN B.3.F.5.c(1) SR-275 Table 34
TA.SP.72	Sensitive data in transit that requires confidentiality protection are encrypted when traversing entity boundaries. For data in transit where the only concern is the protection of integrity, hashing techniques and message authentication codes are used instead of encryption.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include the system of interest demonstrating a plan to use FIPS 140-2 approved or better encryption technology and solution (R1, R2); demonstration of its use (R3) to ensure the proper safeguarding of ePHI/PII. Enterprise: The state must ensure that its business partners and downstream entities are complying with the state's policies in a consistent and effective manner. State should provide audit reports to that effect. Module: This applies to modules that process, store, manage, disclose and use ePHI/PII.	Yes	B.4.D.5 Security IP.5.3 Figure 8 EDW ITN B.3.F.5.c(1) SR-276 Table 34
TA.SP.74	The system of interest uses only FIPS Pub 140-2-approved (or higher) encryption algorithms.	IBP	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include the system of interest demonstrates plan to use FIPS 140-2 approved or better encryption technology and solution (R1, R2), demonstration (R3) to ensure the proper safeguard of ePHI/PII. Enterprise: The state must ensure their business partners and downstream entities are complying with the state's policies in a consistent and effective manner. State should provide audit reports to that effect. Module: This applies to modules that process, store, manage, disclose and use ePHI/PII.	Yes	B.4.D.11 Hosting and Environment IP.11.15 Figure 14 EDW ITN B.3.F.5.c(1) SR-277 Table 34

TA.SP.75	The system of interest employs malicious code protection mechanisms at IT system information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code.	IBP	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include this malicious code protection controls section in SSP (R1, R2), demonstration (R3). Enterprise: The state must ensure their business partners and downstream entities are complying with the state's policies. State should provide audit reports to that	Yes	B.4.D.11 Hosting and Environment IP.11.15 Figure 14
TA.SP.76	The system of interest updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with IT system configuration management policy and procedures.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist. Evidence should include the malicious code protection controls section in SSP (R1, R2, R3) along with evidence that updates and patches have been applied since the go-live date (R2, R3). Enterprise: The state must ensure that its business partners and downstream entities are complying with the state's policies. State should provide audit reports to that effect.	Yes	B.4.D.11 Hosting and Environment IP.11.15 Figure 14 EDW ITN B.3.F.5.c(1) SR-278 Table 34
TA.SP.77	The state and IT solution have implemented to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI in accordance with the HIPAA Security Rule on a control by control basis as defined by the NIST Cybersecurity Framework and NIST SP 800-53.	HIPAA	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist and because of ePHI classification. HHS OCR has provided a mapping between HIPAA Security Rule with NIST Cybersecurity Framework to help entities covered by HIPAA identify potential gaps in their programs. The mapping can be found at https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html. Direct link to mapping (https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf). Evidence	Yes	B.1.D Procurement Library Technology Standards EDW ITN B.3.F.5.c(1) SR-279 Table 34

TA.SP.9	The system must support audit controls for hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	45CFR164.310	For E&E only, the state need not supply evidence for this criterion, provided the state has met the MARS-E criterion in the E&E checklist and because of ePHI classification. Evidence should include this in the system environment - audit and accountability section of SSP (R1, R2, R3). Enterprise: The state must ensure that all modules support audit controls. Module: Modules that contain or use ePHI must include support for audits.	Yes	B.4.D.5 Security IP.5.30 B.4.D.7 Integration IP.7.24 EDW ITN B.3.F.5.c(1) SR-280 Table 34

Information Architecture Checklist

Ref #	System Review Criteria	Source	Guidance	IS/IP Certification Requirement	Project Initiation Milestone Evidence
IA Component Name: Conceptual Data Model (CDM)					
IA.CDM.1	The SMA demonstrates adoption of a CDM that depicts the business area high-level data and general relationships for intrastate exchange.	MITA 3.0 IA ML 3	Enterprise: Evidence would include the enterprise conceptual data model with traceability to the modules' conceptual data models (R1, R2, R3). Modules: Evidence would include a conceptual data model that describes the business area covered by the module's functionality.	Yes	B.1.C.2 Overview of MES Exhibit 2 EDW ITN B.3.F.5.c(2) SR-281 Table 35
IA.CDM.2	The system of interest identifies relationships between key entities in the Medicaid enterprise.	MMIS BP	The key entities are any systems that interface with MMIS or E&E or depend upon data coming from them, even if a digital interface isn't yet in place. Evidence could include plans to map all the relationships (R1) or documentation of the actual relationships (R2, R3). Enterprise: Identify all the entity relationships in the Medicaid enterprise. Modules: Identify the other business area functions with which the module needs to interact.	Yes	B.1.C.2 Overview of MES Exhibit 2 EDW ITN B.3.F.5.c(2) SR-282 Table 35
IA Component Name: Data Management Strategy (DMS)					
IA.DMS.2	The SMA demonstrates adoption of an intrastate metadata repository where the agency defines the data entities, attributes, data models, and relationships sufficiently to convey the overall meaning and use of Medicaid data and information.	MITA 3.0 IA ML 3	Enterprise: Evidence could include plans or designs for the repository, data model, etc. (R1), a list of the metadata captured in the state's Medicaid enterprise metadata repository or screenshots of the repository, etc. (R2, R3). Modules: If COTS, should include proposed metadata for the module (state can choose to adopt them or not). If module developed by state, demonstrate that module uses state's metadata standards.	Yes	B.4.E Procurement Library: MES Data Management Strategy EDW ITN B.3.F.5.c(2) SR-283 Table 35

IA.DMS.4	The SMA demonstrates adoption of statewide standard data definitions, data semantics, and harmonization strategies.	MITA 3.0 IA ML 3	Evidence could include plans in schedule and contracts for setting data standards (R1), data management plan (R2, R3). Enterprise: Provide evidence that it has created standard data definitions and data semantics and that the strategies are being reviewed/updated as modules are added, if necessary, as rules changes, etc. Modules: Demonstrate that the module is using the state's data definitions and semantics.	Yes	B.4.E Procurement Library: MES Data Management Strategy EDW ITN B.3.F.5.c(2) SR-284 Table 35
IA.DMS.5	The system of interest updates all historical claim data, recipient enrollment, provider enrollment, and other primary reference data on a scheduled basis.	MMIS BP	This criterion does not apply to E&E. Evidence could be plans to include as a system requirement (R1), test reports for this functionality (R2), a log of actual updates (R3). Enterprise: All modules update primary reference data regularly. Module: The module demonstrates that it supports regular data	No	EDW ITN B.3.F.5.c(2) SR-285 Table 35
IA Component Name: Data Standards (DS)					
IA.DS.1	The system of interest supports system transmission and receipt of all current version x12N and NCPDP eligibility verification transactions.	HIPAA 5010	This criterion does not apply to E&E. This criterion applies to modules that generate or transform data related to x12N or NCPDP eligibility verification transactions. Evidence could include requirements or plans to test this functionality (R1), test reports or demonstration showing that the module(s) supports these transmission or receipts (R2, R3).	Yes	B.4.D Procurement Library: MES Data Standards
IA.DS.10	The system of interest, at a minimum, supports transfer of data from MMIS and to other entities (e.g., claims history, recipient enrollment, provider enrollment, and primary reference data information (e.g. diagnosis, procedure, national drug code [NDC], and pricing).	MMIS BP	This criterion does not apply to E&E. Evidence could include plans to include this capability (R1), test reports (R2), or demonstration of data transfer (R2, R3). Modules: Applies to modules involved in any aspect of transferring data to other entities.	Yes	B.1.C.2 Overview of MES Exhibit 2 Procurement Library: MES Data Standards EDW ITN B.3.F.5.c(2) SR-286 Table 35

IA.DS.11	The system of interest supports consumption of data in multiple formats from many sources, such as vital statistics, MCO encounter data, benefit manager encounter data (pharmacy, dental, mental health), waiver program data, and census bureau.	MMIS BP	This criterion does not apply to E&E. Enterprise: Evidence could include plans (ConOps, Data Management Plan, etc.) to develop this capability (R1), and test reports and demonstrations (R2, R3). Modules: Evidence could include test reports showing that the module(s) accepts data in multiple formats from various sources, relevant to the scope of the module's intended functionality.	Yes	B.1.C.2 Overview of MES Exhibit 2 Procurement Library: MES Data Standards EDW ITN B.3.F.5.c(2) SR-287 Table 35
IA.DS.12	The system of interest supports sending electronic claim payment/advice transactions (ASC X12N 835) meeting the standards required by 45 CFR Part 162.	HIPAA	This criterion does not apply to E&E. Evidence could include requirements or plans to develop this capability (R1) and test reports or demonstration (R2, R3) showing that the module(s) supports these transmission or transformations. Enterprise: This applies to modules that generate or transform data related to claim payment/advice transactions (ASC X12N	Yes	B.4.D.7 Integration
IA.DS.13	The system of interest requires, captures, and maintains the 10-digit national provider identifier.	HIPAA	This criterion does not apply to E&E. Modules: This criterion applies to modules that use the 10-digit national provider identifier. Evidence could include requirements or plans to develop this capability (R1) and test reports or demonstration (R2, R3) showing that the module(s) appropriately captures and maintains the identifier.	Yes	B.4.D.6.b Master Data Management IP.6.27 Exhibit 10 EDW ITN B.3.F.5.c(2) SR-288 Table 35
IA.DS.14	The system of interest accepts the national provider identifier in all standard electronic transactions mandated under HIPAA.	HIPAA	This criterion does not apply to E&E. Evidence could include requirements or plans to develop this capability (R1) and test reports or demonstration (R2, R3) showing that the module(s) accept the national provider identifier as part of these transactions. This criterion applies to modules that participate in any HIPAA-mandated transactions.	Yes	B.4.D.6.b Master Data Management IP.6.27 Exhibit 10 EDW ITN B.3.F.5.c(2) SR-289 Table 35

IA.DS.15	The system of interest interfaces with the National Plan and Provider Enumerator System (NPPES) to verify the NPI of provider applicants.	HIPAA	This criterion does not apply to E&E. Evidence could include requirements or plans to develop this capability (R1) and test reports or demonstration (R2, R3) showing that the module(s) interface with these databases. This criterion applies to modules that should interface with the National Plan and/or Provider Enumerator System (NPPES).	Yes	B.4.D.6.b Master Data Management Exhibit 10
IA.DS.16	The system of interest does not allow atypical providers to be assigned numbers that duplicate any number assigned by the NPPES.	HIPAA	This criterion does not apply to E&E. Evidence could be plans to include duplication checks (R1), duplication check test results showing that the module does not assign a number that duplicates an existing NPPES number (R2, R3). State should design its number scheme such that it eliminates the chance of having duplicates with NPPES (even in the future). No module should be capable of assigning numbers to providers that duplicate any number assigned by NPPES.	Yes	B.4.D.6.b Master Data Management Exhibit 10 EDW ITN B.3.F.5.c(2) SR-290 Table 35
IA.DS.17	The system of interest provides ability to link and de-link to other Medicaid provider IDs for the same provider, (e.g., numbers used before the NPI was established, erroneously issued prior numbers, multiple NPIs for different subparts, etc.). Captures/crosswalks subpart NPIs used by Medicare (but not Medicaid) to facilitate coordination of benefits (COB) claims processing.	HIPAA	This criterion does not apply to E&E. Evidence could include requirements or plans to develop this capability (R1) and test reports or demonstration (R2, R3) showing that relevant modules are able to associate and de-associate a provider to his/her identifiers other than the NPI identifier.	Yes	B.4.D.6.b Master Data Management Exhibit 10
IA.DS.18	The system of interest is capable of or supports the production of a random sample of data that would be needed for audit purposes (e.g., providers, beneficiaries, claims, etc.) based on the state-established selection criteria.	IBP	This criterion does not apply to E&E. Evidence could be plans to include this functionality (R1) and for R2 and R3 a randomly generated list (e.g., provider type, year-to-date reimbursement, etc.) or a demonstration of the functionality. Enterprise: The state is able to generate a random sample of providers. Modules: This criterion applies only to modules that maintain the authoritative provider data	No	EDW ITN B.3.F.5.c(2) SR-291 Table 35

IA.DS.19	The system of interest processes or supports actions and responses to B Notices from Internal Revenue Service (IRS) as determined by the state.	IBP	Evidence could be plans to include this functionality (R1) and test reports or demonstrations (R2 and R3). States: The MMIS responds appropriately to B Notices. The actions necessary to support this may span more than one module. Module: This criterion applies only to modules that support responses to B Notices.	No	This functionality with be part of a future Financial Module with letter generation through common services.
IA.DS.2	The system of interest supports production of X12N 270 transactions to query other payer eligibility files and ability to process responses.	HIPAA 5010	This criterion does not apply to E&E. Evidence could be plans to include this functionality (R1) and test reports or demonstrations (R2 and R3). Enterprise: The MMIS produces the transactions and processes responses. The actions necessary to support this may span more than one module. Modules: This criterion applies only to modules that support X12N 270 transactions.	Yes	B.4.D.7 Integration
IA.DS.21	The system of interest maintains all HIPAA-required data sets (e.g. ICD-10, NDC), including those defined by the HIPAA implementation guides to support all transactions required under HIPAA administrative simplification rule (e.g., gender, reason code).	HIPAA	This criterion does not apply to E&E. Evidence could be plans to include the HIPAA data sets (R1), the data dictionary, and test reports showing that the ICD-10 transition was performed successfully (R2, R3). Enterprise: The state has a data dictionary. Modules: This criterion applies only to modules that maintain HIPAA-required data sets.	No	EDW ITN B.3.F.5.c(2) SR-292 Table 35
IA.DS.5	The system of interest supports the sending and receiving of electronic claims transactions, containing valid codes, required by 45 CFR Parts 160 and 162, as follows: • Retail pharmacy drug claims (NCPDP) • Dental health care claims (X12N 837D)	45 CFR, 160 and 162	This criterion does not apply to E&E. Evidence could be plans to include functionality (R1), and integration test reports or demonstration (R2, R3). Enterprise: The MMIS is able to send and receive NCPDP and X12N 837D transactions across the relevant modules. Modules: This criterion applies only to modules that support send/receive functionality for NCPDP and X12N 837D claims transactions.	Yes	B.4.D.7 Integration EDW ITN B.3.F.5.c(2) SR-293 Table 35

IA.DS.6	The system of interest provides secure, HIPAA-compliant software and documentation for use by providers to submit electronic claims.	HIPAA	This criterion does not apply to E&E. Evidence could include plans to test (R1), test results that demonstrate HIPAA compliance (R2), and attestation of compliance (R3). Enterprise and modules: Comply with all HIPAA regulations. Modules that provide interfaces to providers or receive information from them must demonstrate that the modules are secure and HIPAA compliant.	Yes	B.4.D.14 Performance Standards IP.14.13 Figure 17 B.4.E.9 IS.8.6 Exhibit 26
IA.DS.7	The system of interest processes batch 837 claims, rejecting only individual bad claims and accepting all others.	IBP	This criterion does not apply to E&E. Evidence could be interface and integration plans (R1), test reports (R2), demonstration of the functionality (R3). Enterprise: The MMIS is able perform the batch 837 claims jobs. For modules: This applies only to modules that process batch 837 claims. Evidence could be test results that demonstrate ability to support these transactions.	No	Functionality will the part of a potential Core Module that handles claims processing.
IA.DS.9	The system of interest complies with the SMA's standardized structure and vocabulary data for automated electronic intrastate interchanges and interoperability.	MITA 3.0 IA ML3	Evidence could be state's interoperability standards (R1), test reports for its usage (R2), and demonstration of the functionality (R3). Enterprise: Has standardized structure and vocabulary data standards. Show how they are being used by the modules. Module: Show use of the SMA's documented standards for interoperability.	No	EDW ITN B.3.F.5.c(2) SR-294 Table 35
IA Component Name: Logical Data Model (LDM)					
IA.LDM.1	The system of interest accepts, records, stores, and retrieves documents (free-form or in HIPAA attachment format) submitted with or in reference to claim submission activity, and auto-archives or forwards to appropriate operational area for processing.	IBP	This criterion does not apply to E&E. This criterion applies to modules that intake claims. They should be able to attach and retrieve claims-related documents such as operative reports; occupational, physical, and speech therapy reports; durable medical equipment and warranty data; manufacturer's tracking data for implants; waivers and demonstration-specific requirements; etc. Evidence could include plans to include this capability (R1), test reports (R2), and a few samples of claims with HIPAA-compliant attachments (R3).	Yes	B.4.D.3 Managed File Transfer EDW ITN B.3.F.5.c(2) SR-295 Table 35
IA.LDM.3	The system of interest associates clinical data (e.g., claims attachment) with the claim record.	IBP	This criterion does not apply to E&E. This applies only to modules that associate clinical data to claims. Evidence could be plans to develop the capability (R1), test reports of the functionality (R2), and demonstration of the function (R3).	No	EDW ITN B.3.F.5.c(2) SR-296 Table 35

IA.LDM.4	The system of interest maintains synchronization of claims and encounter record dates with provider and member record dates (i.e. a claim or encounter is always linked to the provider status and member status segments associated with the date of service).	MMIS BP	This criterion does not apply to E&E. Evidence could be plans to develop the capability (R1), test reports of the functionality (R2) and demonstration of the function (R3). Enterprise: Ensure that synchronization is occurring across relevant modules to provide this functionality. Modules: This applies to any module involved in providing information needed to synchronize claims and encounter records.	No	EDW ITN B.3.F.5.c(2) SR-297 Table 35
IA.LDM.5	The system of interest Logical Data Model (LDM) supports identification of data classes, attributes, relationships, standards, and code sets for intrastate exchange.	MITA 3.0 IA ML 3	Evidence could include data modeling plans (R1), test reports (R2, R3), and attestation (R3). Enterprise: Needs to have a thorough logical data model. Modules: Must use the state LDM for their physical data model.	Yes	B.1.D Procurement Library Technology Standards EDW ITN B.3.F.5.c(2) SR-298 Table 35
IA.LDM.6	The system of interest maintains providers' data (e.g., links from providers to other entities, such as groups, managed care organizations, chains, networks, ownerships, and partnerships).	SMM	This criterion does not apply to E&E. Evidence could include plans to include linkages (R1), test reports (R2), and demonstration (R3). Enterprise: Ensure that linkages are valid across all relevant modules. Modules: This applies only to modules involved in maintaining provider data.	No	EDW ITN B.3.F.5.c(2) SR-299 Table 35
S&C.IC.3	The system conforms to ASC X12 Technical Reports Type 3 (TR3), Version 005010 is mandated by 1/1/2012.		This criterion does not apply to E&E. Evidence can include design and requirements (R1) and transaction data (R2, R3). Module: This only applies to modules that are related to TR3 types--they must support ASC X12.	Yes	B.4.D.7 Integration EDW ITN B.3.F.5.c(2) SR-300 Table 35

TA.SP.1	The system of interest verifies that all fields defined as numeric contain only numeric data.	SMM	Evidence could include plans to test this (R1) and test reports (R2, R3). Enterprise: Ensure that this criterion applies across all relevant modules. Modules: Ensure that malicious code cannot be placed into fields.	Yes	B.4.D.11 Hosting and Environment IP.11.15 Figure 14 EDW ITN B.3.F.5.c(2) SR-301 Table 35
TA.SP.12	The SMA adopts CAQH CORE Phase I, II and III as stipulated in 45 CFR 162 (Operating Rules for HIPAA Transactions).	45CFRP162.1403	This criterion does not apply to E&E. Evidence could include state policies (R1) and test reports (R2, R3). Enterprise: Ensure that this criterion applies across all relevant modules. Modules: Applies to modules that perform HIPAA	No	EDW ITN B.3.F.5.c(2) SR-302 Table 35
TA.SP.16	The system of interest supports ANSI X12N 820 Premium Payment transaction as required by HIPAA.	HIPAA	This criterion does not apply to E&E. Evidence could include state policies (R1) and test reports (R2, R3). Enterprise: Ensure that this criterion applies across all relevant modules. Modules: Applies to modules that perform X12N 820 transactions.	Yes	B.4.D.7 Integration
TA.SP.17	The system of interest supports all ANSI X12N transactions as required by HIPAA.	HIPAA	This criterion does not apply to E&E. Evidence could include state policies (R1) and test reports (R2, R3). Enterprise: Ensure that this criterion applies across all relevant modules. Modules: Applies to modules that perform X12N transactions.	Yes	B.4.D.7 Integration
TA.SP.2	The system of interest verifies that all fields defined as alphabetic contain only alphabetic data.	SMM	Evidence could include plans to test this (R1) and test reports (R2, R3). Enterprise: Ensure that this criterion applies across all relevant modules. Modules: Ensure that malicious code cannot be placed into fields.	Yes	B.4.D.11 Hosting and Environment IP.11.15 Figure 14 EDW ITN B.3.F.5.c(2) SR-303 Table 35

Integration and Utility Checklist

Ref #	System Review Criteria	Source	Guidance	IS/IP Certification Requirement	Project Initiation Milestone Evidence
Technical Service Classification: Configuration Management					
TA.CM.4	The system of interest uses technology-neutral interfaces that localize and minimize impact of new technology insertion.	MITA 3.0 TCM ML2	This criterion addresses the use of modern principles and protocols implemented through open web services and APIs. Evidence could include plans and designs to implement technology-neutral interfaces (R1), test reports of successful information exchange using the interfaces (R2), and attestation of their use (R3). Module: demonstrate use of APIs.	Yes	B.4.D.1 Enterprise Service Bus EDW ITN B.3.F.5.c(3) SR-304 Table 36
Technical Service Classification: Data Access and Management					
TA.DAM.1	The system of interest maintains online access to at least four years of selected management reports and five years of annual reports.	IBP	Evidence could include policies (R1), requirements and test reports (R2, R3), showing ability to pull reports for prior four or five years. Enterprise: The state has data retention policies reflected in contracts and in practice that require at least four years of state-stipulated and CMS-required management reports and five years of annual reports. Module: The module demonstrates that it passes its data to enterprise data store through defined APIs.	Yes	B.6.A General Reporting Requirements EDW ITN B.3.F.5.c(3) SR-305 Table 36
TA.DAM.2	The system of interest conducts information exchange (internally and externally) using MITA Framework, industry standards, and other nationally recognized standards.	MITA 3.0 TCM ML3	Evidence could include a statement in the ConOps as to which standards the state will use (R1), test reports of successful information exchange using the standards (R2, R3), and attestation of their use (R3). State and modules: Evidence should show how the solution uses nationally recognized standards adopted by the state.	Yes	B.4.D.7 Integration Requirements Figure 10 EDW ITN B.3.F.5.c(3) SR-306 Table 36

TA.DAM.3	The system of interest develops data models that include mapping of information exchange with external organizations.	MITA 3.0 TCM ML2	Evidence could be plans to develop the data model (R1), and the data model (R2, R3). Enterprise: The state's data models cover MMIS / E&E enterprise. Modules: The module has identified which data can be shared externally and enables sharing of that data.	Yes	B.4.D.7 Integration Requirements Figure 10 EDW ITN B.3.F.5.c(3) SR-307 Table 36
TA.DAM.7	The system of interest applies single source of information methodologies.	MITA 3.0 TCM ML2	For each data element there is an identified, authoritative source. Evidence would include documentation of the system of record for each data element.	Yes	B.4.D.6 Master Data Management EDW ITN B.3.F.5.c(3) SR-308 Table 36
Technical Service Classification: Decision Management					
TA.DM.1	The system of interest uses standardized business rules definitions that reside in a separate application or rules engine.	MITA 3.0 TCM ML3	"Standardized" in this context means rules derived from the SMM and the state's documented business rules. Rules must not be hard coded into modules' code. Evidence could include plans to acquire a business rules engine (R1), and screenshots and demonstrations of its use (R2, R3).	Yes	IS/IP ITN - B.12 Federal Certification Procurement Library: IS/IP MMIS Core Certification Checklist B.4.D.4 Business Rules Engine
TA.DM.2	The system of interest uses rules editor that maintains the current version of standardized business rules definitions in a language that business people can interpret and transforms them into machine language to automate them.	MITA 3.0 TCM ML3	State and modules: Evidence could include plans to ensure business rules are defined so that stakeholders can understand them (R1) and the business rules definitions alongside the corresponding natural language, test reports, or demonstrations of the rules editor (R2, R3).	Yes	IS/IP ITN - B.12 Federal Certification Procurement Library: IS/IP MMIS Core Certification Checklist B.4.D.4 Business Rules Engine
Technical Service Classification: Logging					

TA.LG.1	The authorized user has access to user activity history and other management functions, including log-on approvals/ disapprovals and log search and playback.	MITA 3.0 TCM ML2	Evidence could include plans to include this capability (RFPs, high-level requirements, etc.) (R1) and logs of a user's activity (R2, R3). Modules: Every module should support this capability. The intent of this criterion is to ensure that the state can perform audits and can report which users and non-permissioned users accessed what screens and data and when. These logs should also record what unsuccessful attempts were made to access data and by whom. The state should have a retention period sufficient to perform audits and reviews and ensure that all modules comply with the	Yes	EDW ITN B.3.F.5.c(3) SR-309 Table 36 IS/IP ITN B.4.D.5 IP.5.2 Figure 8
TA.LG.2	The system of interest defines information sharing and event notification standards to allow aggregated and integrated information.	MITA 3.0 Part III, Ch. 4 and 7.	Evidence could include plans to include this capability (R1), documentation of notification standards used, test reports (R2) and attestation (R3) regarding their use. State: Defines standards for sharing information and event notification. Modules: Leverage standardized framework of registration, messaging, and discovery. Register with framework and use discovery mechanism and use standard messaging capabilities to send its event messages.	Yes	IS/IP ITN - B.12 Federal Certification Procurement Library: IS/IP MMIS Core Certification Checklist B.4.D.1 Figure 4

Intermediary and Interfaces Checklist

Ref #	System Review Criteria	Source	Guidance	IS/IP Certification Requirement	Project Initiation Milestone Evidence
Technical Service Classification: Business Process Management					
TA.BPM.1	The system of interest uses Enterprise Content Management (ECM) services to allow entry of different forms of information content in a variety of ways.	MITA 3.0 Part III, Ch5 Application Architecture	This criterion applies to the enterprise, as individual modules do not provide their own ECMs. The state should implement a true ECM service. Evidence could include plans to use ECM (R1), and test reports and demonstrations (R2, R3).	No	EDW ITN B.3.F.5.c(4) SR-310 Table 37
TA.BPM.4	The system of interest uses a mix of manual and automated business processes.	MITA 3.0 TCM ML2	This criterion applies to the enterprise. Evidence should demonstrate that the system uses at least some process automation (for example, show BPEL for a few automated processes). Evidence could include plans to use this capability (R1), test reports (R2), and attestation (R3).	Yes	B.4.D.1 Enterprise Service Bus IP.1.16 Figure 4 EDW ITN B.3.F.5.c(4) SR-311 Table 37
Technical Service Classification: Data Connectivity					
TA.DC.1	The system receives and processes member eligibility information from external sources.	SMM	Enterprise: This applies to receiving information from sources such as a state's integrated eligibility system or SSA's State Data Exchange. Capabilities should include 1) ability to produce comprehensive and detailed information that supports error correction and synchronization, 2) applying reconciliation changes to master file, 3) producing a file of changed records, and 4) sending the file of changed records to the originating source. Evidence could include plans to include this capability (R1), test reports (R2), and attestation (R3). Module: This applies only to modules that support the receiving and processing of this data.	Yes	B.20 External Stakeholders Exhibit 34

TA.DC.10	The system of interest securely conducts electronic information exchange within the agency and with multiple intrastate agencies via an information hub.	MITA 3.0 TCM ML3	Evidence could include plans to include this capability (R1), test reports and demonstrations (R2, R3). Enterprise: State should ensure modules and other state systems are exchanging information properly. Module: Should have capability to send / receive data through the enterprise from other state systems.	Yes	B.4.E Procurement Library: MES Data Management Strategy
TA.DC.3	Assure adjudication for payment within 30 days after receipt of any properly submitted correct claim which passes all required edits and checks.	SMM	This criterion does not apply to E&E. Evidence could be inclusion of this requirement in development and test plans (R1), test reports (R2), error reports (are claims being incorrectly flagged as erroneous?) (R3), and reports showing time it takes to adjudicate claims (dental, medical, pharmacy, etc.) (R3). Enterprise: State must ensure that end-to-end process across all relevant modules for paying claims does not exceed 30 days from claim receipt. Module: Modules that handle error flagging must correctly flag claims with errors. Modules that handle adjudication and payment processing must do so in order that the overall payment is not delayed.	No	Functionality will be part of a potential Core Module for claims processing.
TA.DC.5	The system of interest interfaces with the pharmacy prior authorization database.	SMM, CFR	This criterion does not apply to E&E. Evidence could include plans to include this capability (R1), SDD, test reports, and demonstrations (R2, R3). Enterprise: State should have designs that indicate which modules will need to interface with the pharmacy prior authorization database. Module: This applies only to modules that should interface with the pharmacy prior authorization database.	Yes	B.4.E.2 Procurement Library: MES Data Management Strategy
TA.DC.6	The system interfaces with electronic authorization for retail pharmacy drug referral certification and authorization.	HIPAA; 45 CFR Part 162	This criterion does not apply to E&E. Evidence could include plans to include this capability (R1), SDD, test reports, and demonstrations (R2, R3). Enterprise: The state should ensure that the relevant interfaces between the relevant modules are working. Module: This applies only to modules that support pharmacy drug referrals and authorizations.	Yes	B.4.E.2 Procurement Library: MES Data Management Strategy

TA.DC.7	The system of interest performs advanced information monitoring and routes system alerts and alarms to communities of interest when the system detects unusual conditions.	MITA 3.0 TCM ML3	Evidence could include plans to include operational monitoring and alerting triggers (R1), event logs, alerts, and escalation protocols (R2, R3). Enterprise: The IT solution performs advanced information monitoring and routes system alerts and alarms to communities of interest if the system detects unusual conditions. Module: Consider if the module in question functions in such a manner that any inherent failure or error event would have a direct impact on some other element of the overall system.	Yes	EDW ITN B.3.F.5.c(4) SR-314 Table 37 IS/IP ITN B.4.D.5 IP.5.17 Figure 8
TA.DC.9	The system of interest uses XML standards for message format to ensure interoperability.	MITA 3.0, Part III Ch2, Tech Mgmt Strategy	Evidence could include plans to use XML in RFPs and/or ConOps (R1), and samples of XML messaging (R2, R3). This criterion applies across the enterprise and for individual modules.	Yes	B.4.D.1 Enterprise Service Bus IP.1.15 Exhibit 5
Technical Service Classification: Service Oriented Architecture					
TA.SOA.1	The system of interest adopts MITA-recommended ESB, automated arrangement, coordination, and management of system.	MITA 3.0 TCM ML3	This criterion means that the Medicaid system uses an ESB. Evidence could include plans to have an ESB (R1), and enterprise system diagrams such as are found in System Design Document (R2, R3) and test reports and demonstrations showing that individual modules are successfully integrated with the ESB. Module: Modules should be configurable to plug into the state's ESB.	Yes	B.4.D.1 Enterprise Service Bus Exhibit 5
TA.SOA.2	The system of interest conducts reliable messaging, including guaranteed message delivery (without duplicates) and support for non-deliverable messages.	MITA 3.0 TCM ML2	Evidence could include plans to include this functionality (R1), enterprise system diagrams such as are found in System Design Document, including how the state guarantees message delivery and test reports (R2, R3). Module: This criterion applies to any modules responsible for messaging.	Yes	B.4.D.1 Enterprise Service Bus Exhibit 5

TA.SOA.4	The SMA conducts system coordination between intrastate agencies and some external entities. Otherwise, we can change it in the later version.	MITA 3.0 TCM ML3	This criterion means that the system interfaces or integrates with at least some external or intrastate agencies. Evidence could include list of external agencies the system coordinates and by what methods in the ConOps and ICD documents (R1), and test reports and demonstrations (R2, R3). Enterprise: State should ensure that stakeholder and technical coordination is happening across all relevant modules and the external entities. Module: Applies only to modules that interface with external / intrastate entities.	Yes	B.4.E.2 Interface Integration
Technical Service Classification: System Extensibility					
TA.SE.2	The system of interest uses RESTful and/or SOAP-based web services for seamless coordination and integration with other U.S. Department of Health & Human Services (HHS) applications and intrastate agencies, including the Health Insurance Exchange (HIX).	MITA 3.0 TCM ML3	Evidence could include ConOps (R1) and enterprise design diagrams (R2, R3). Enterprise: State should Module: This criterion applies to modules that must integrate with HHS and intrastate agencies.	Yes	B.4.D.1 Enterprise Service Bus IP.1.15 Exhibit 5
TA.SE.3	The system of interest documents all interfaces in an Interface Control Document (ICD), along with how those interfaces are maintained.	IBP	Evidence could include ConOps, ICDs, or System Design Document (R1, R2, R3). Enterprise: State should ensure that all system interfaces between modules with external entities are defined and maintained. Module: Define capabilities for interfacing with other modules or external entities, identify what modules / capabilities it should interface with, and how it will do so.	Yes	EDW ITN B.3.F.5.c(4) SR-313 Table 37 IS/IP ITN B.4.D.7 IP.7.8 Figure 10

Standards and Conditions Checklist

Ref #	System Review Criteria	Source	Guidance	IS/IP Certification Requirement	Project Initiation Milestone Evidence
S&C: Business Results Condition					
S&C.BRC.5	The system of interest accommodates customer preferences for communications by email, text, mobile devices, or phones.	MITA level 3	This applies to modules that have user-facing interfaces. Evidence could include plans to include this capabilities (R1), requirements documents and test reports (R2), or demonstration (R3).	Yes	Module Specific
S&C: Industry Standards Condition					
S&C.ISC.6	The system of interest complies with standards and protocols adopted by the Secretary under sections 1104 and 1561 of the Affordable Care Act.	Sect 1561 and 1104 of ACA	This criterion speaks to health information enrollment standards and protocols to promote the interoperability of systems for enrollment of individuals in federal and state health and human services programs as well as adoption of uniform standards and operating rules for the electronic transactions that occur between providers and health plans that are governed under the HIPAA. Establishes a process to regularly update the standards and operating rules for electronic transactions and requires health plans to certify compliance or face financial penalties. The goal of this section is to make the health system more efficient by reducing the clerical burden on providers, patients, and health plans. Evidence: Concept of Operations (R1), test reports (R2), and demonstration of data exchange (R3). Enterprise: State should have an architecture that supports this capability. Module: This applies only to modules involved in data exchange with human services systems. These should be able to support the state's data exchange goals.	Yes	B.4.D.14 Performance Standards Figure 17
S&C: Interoperability Condition					

S&C.IC.2	SMA uses a medical code set for coding diseases, signs and symptoms, abnormal findings, and external causes of injuries/diseases, as stipulated in 45 CFR Part 162.1002.	45 CFR Part 162	This criterion does not apply to E&E. The state Medicaid IT system uses the currently HHS-mandated codes sets, including pharmaceutical codes, diagnosis codes, etc. Evidence could include the state's policy regarding code sets and a data dictionary (R1,R2), and test reports (R3). Enterprise: State should have documentation stating which code sets will be used. Module: Modules must accommodate usage of the mandated code sets.	No	EDW ITN B.3.F.5.c(5) SR-314 Table 38
S&C.IC.4	The system uses the Clinical Modification (ICD–10 CM) for diagnosis coding (including the Official ICD–10 CM Guidelines for Coding and Reporting), and, the Procedure Coding System (ICD–10 PCS) for inpatient hospital procedure coding (including the Official ICD–10 PCS Guidelines for Coding and Reporting).	CMS 0013F 45 CFR, parts 160, 162, and, Protecting Access to Medicare Act (PAMA) of 2014; HHS Final Rule	HIPAA-covered entities were authorized to process and adjudicate claims using ICD-9 code sets up to and including 9/30/2015. On 10/1/2015, HIPAA-covered entities are authorized to process and adjudicate claims using the ICD-10 code set. This criterion does not apply to E&E. Evidence could include plans to use ICD-10 (R1) and test reports and demonstration of its use along with the ability to access old claims that use ICD-9 (R2, R3). Module: For modules that use ICD codes, the module can support import of legacy (ICD-9) data using a ICD-9/ICD 10 mapping function provided by the state.	No	EDW ITN B.3.F.5.c(5) SR-315 Table 38
S&C.IC.6	The architecture adopted preserves the ability to efficiently, effectively, and appropriately exchange data with other participants in the health and human services enterprise.	IBP	This criterion speaks to integration with programs like SNAP, TANF, etc. Evidence: Concept of Operations (R1), test reports (R2), and demonstration of data exchange (R3). Enterprise: State should have an architecture that supports this capability. Module: This applies only to modules involved in data exchange with human services systems. These should be able to support the state's data exchange goals.	Yes	EDW ITN B.3.F.5.c(5) SR-316 Table 38
S&C: Leverage Condition (Reuse)					

S&C.LC.11	SMA has identified and adopted transition and retirement plans.	MITA level 4	Evidence could include an SDLC with a retirement phase included (R1), transition and retirement plans (R2, R3). Enterprise: State should have a comprehensive and integrated view of when each module in its enterprise is no longer likely to be supported by the vendor. Transition and retirement plans should include length of support for all modules. Module: Vendors should indicate how long they intend to support their product versions (paths, configuration, etc.) so that the state can plan for transition and retirement of modules.	Yes	B.4.E.11 IS/IP Turnover EDW ITN B.3.F.5.c(5) SR-317 Table 38
S&C: Modularity Standard					
S&C.MS.10	The SMA uses regionally standardized business rule definitions in both human and machine-readable formats.	MITA level 4	Evidence could include plans to discover, document, and test business rules (R1), requirements traceability matrix and test reports (R2, R3). Enterprise: The state should document acceptable technology (e.g. XML) and be able to show business rules management from requirements through test and management. Modules: Each module should show how it is conforming to the state's standards for business rules.	Yes	B.4.D.4 Business Rules Engine Figure 7
S&C.MS.14	The SMA defines system of interest modules that can be interchanged without major system design.	MITA level 3	Evidence could include high-level architecture design, ConOps, and acquisition strategy (R1), SDD, ICD, or other detailed designs that include interoperability standards adopted by the state (R2, R3). Enterprise: The state needs to develop a system architecture that delineates which modules will perform which functions, along with API and interoperability standards the state is adopting. Module: Conforms to state's design in the SDD and ConOps and supports modular architecture through the use of published data dictionary, APIs.	Yes	B.4.E.1 System Interoperability EDW ITN B.3.F.5.c(5) SR-318 Table 38
S&C.MS.16	The state uses an intrastate rules engine separate from core programming with established interstate standardized business rules definitions.	MITA ML3, SS-A Appendix A	"Standardized" in this context means rules derived from the SMM and the state's documented business rules. Rules must not be hardcoded into modules' code. Evidence could include plans to acquire a business rules engine that spans intrastate systems (R1), and screenshots and demonstrations of its use (R2, R3).	Yes	B.4.D.4 Business Rules Engine Figure 7

S&C.MS.18	The system of interest design documents utilize a widely supported modeling language (e.g., UML, BPMN).	MITA level 3	Enterprise and module: Evidence would be design documents that use UML or BPN (R1, R2, R3).	Yes	B.10.C.4 System Design Documents EDW ITN B.3.F.5.c(5) SR-319 Table 38
S&C.MS.2	Open standards between key interfaces have been considered for all and chosen where feasible.	MITA level 3	Evidence could include acquisition documents and designs that stipulate the use of open standards for interfaces (R1), detailed designs that include interoperability standards adopted by the state and test reports showing successful integration between modules (R2, R3). Enterprise: During acquisition planning the state needs to ensure that the modules it acquires will interface properly with each other using open interfaces and not proprietary ones. Module: Show that the module uses the open standards adopted by the state.	Yes	B.1.D Procurement Library: MES Technical Management Strategy EDW ITN B.3.F.5.c(5) SR-320 Table 38
S&C.MS.4	Modularity will be verified through extensive testing that demonstrates compliance with chosen interface standards and specifications.	MITA level 3	Evidence could include acquisition documents requiring integration and interface testing across modules (R1), test results and demonstration (R2, R3). Enterprise: State needs to ensure thorough testing is done with each new module added--does the module properly communicate with all the existing modules? Module: Module has been tested and uses the interface standards and specifications properly.	Yes	B.4.D.8 Testing Requirements Exhibit 12 B.4.E.5 Exhibit 22 EDW ITN B.3.F.5.c(5) SR-321 Table 38