# Statement of Objectives (SOO) – ClaimsCore Program

Prepared by:
Centers for Medicare & Medicaid Services (CMS)
The Center for Medicare (CM)
The Digital Service at CMS (DSAC)
United States DOGE Service (USDS)

Table of Contents

## Vision

The ClaimsCore program seeks to re-platform Medicare Fee for Service claims processing by replacing legacy "Shared Systems" including the Multi-Carrier System (MCS), Fiscal Intermediary Shared System (FISS) and Durable Medical Equipment Claims System (DME) as well as the Common Working File (CWF) with a flexible and interoperable platform that reduces administrative burden and sets improvement of the beneficiary experience as the program's guiding objective. CMS intends to procure a Software as a Services (SaaS) Commercially-Available-Off-The-Shelf (COTS) product and complimentary configuration and integration services that will provide CMS with near real-time adjudication and claims status, policy agility, industry leading enterprise tools, improved fraud prevention capabilities, and tighter integration across CMS, Medicare Administrative Contractor (MACs), providers, and partners.

### Objectives

1. **Replace Shared Systems and the Common Working File (CWF):** Replace FISS, MCS, DME, and CWF with an enterprise class, near real-time platform while maintaining uninterrupted Medicare Fee-for-Service operations during transition. Such a replacement will significantly improve the way Original Medicare does intake, eligibility and coverage checks, edit/rules execution, payment determination, EOB/EOP generation, adjustments and reprocessing, reporting, and audit/traceability, analytics etc.
2. **Beneficiary Transparency and Timeliness**: Enable near real-time adjudication and claims status, faster explanations of benefits, and better visibility into beneficiary responsibility.
3. **Reduce Provider Burden**: Reduce provider burden through increased transparency and consistency, increased automation, and improved revenue certainty.
4. **Fraud, Waste and Abuse (FWA) reduction (i.e., Payment Integrity)**: Speed and flexibility in designing and implementing pre-payment risk scoring and edits, improved payment accuracy, auditing, and anomaly detection to prevent improper payments and protect beneficiaries and taxpayers.
5. **Policy Agility and Flexibility**: Configuration-driven rules to evaluate, back test, quantify impact, and implement new and alternative payment models without long development cycles.
6. **Provider transparency & efficiency**: Comprehensive APIs and interfaces that provide real-time claims status, surface underlying data, allow MAC-operated systems to interact with claims, and reduce provider burden.
7. **Risk Management of Platform Obsolescence**: Full retirement of COBOL mainframe systems and the Common Working File with near real-time, performant, scalable, maintainable, well-supported systems.
8. **High Availability (HA) and Scale:** Target 99.9% uptime with elastic scaling at current and future volumes, eliminating nightly downtimes and "dark days".
9. **Consolidated Development and Operations:** A single unified system for all Original Medicare claims processing, instead of four separate bespoke systems that are further split into separate regions, will lead to more consistent and efficient policy implementation, and to improved analytics and observability of business operations.

10. **Disaster Recovery (DR) and Business Continuity Plans (BCP):** Provide mission-critical DR and BCP for the ClaimsCore solution with defined RTO/RPO objectives and regular failover/DR drills aligned to CMS enterprise continuity plans.
11. **Interoperability**: HIPAA X12, REST/FHIR APIs, and custom flat files integrate efficiently across CMS, MACs, clearinghouses, and provider systems.

### Benefits for Medicare Beneficiaries

The current COBOL systems limit CMS' ability to deploy industry standard tools that improve the beneficiary experience. ClaimsCore will deliver improvements to the Original Medicare experience and provide the underlying platform that can enable follow on technology investments. As ClaimsCore deploys, beneficiaries will see faster claims resolution and stronger fraud protection. As providers adopt new APIs, beneficiaries will gain clearer cost and coverage information at the point of care, including accurate out-of-pocket estimates and digital access to claims and explanations. Over time, ClaimsCore will reduce confusion and surprise billing and creates the foundation for a Medicare experience that more quickly adapts to the needs of Medicare beneficiaries and our nation.

## Context

**Current Environment**: FISS, MCS, DME, and CWF process ~1.2 billion claims annually (≈$460B+). Hosted in CMS Virtual Data Centers, they run on COBOL, Assembler Language Code (ALC), and IBM mainframes. The current Shared Systems and the Common Working File (CWF) present significant challenges, including claims processing delays, code and policy audit challenges, outdated code bases that hinder policy changes, inflexible external systems integration, limited data transparency across contractor regions, an aging COBOL workforce, and expensive maintenance of mainframe environments. The Shared Systems and CWF's siloed and centralized architecture constrain scalability and complicates integration with modern data standards, making real-time analytics and interoperability with external systems difficult. These issues collectively slow innovation, increase administrative burden, and limit CMS's ability to implement new payment models efficiently.

**Stakeholders**: Within CMS, the ClaimsCore program is led by the Digital Services at CMS (DSAC) organization, sponsored by CM, Office of Information Technology (OIT), and Office of the Administrator (OA), and engages nearly all Medicare related offices, with MACs and providers as critical partners. Providers and beneficiaries will benefit from faster, more transparent claims, and reduced administrative burden while other CMS offices will use the platform for program integrity, payments, and policy implementation and evaluation.

## Statement of Need

### Challenges with MCS, FISS, DME, and CWF

**1. Policy change agility**

CMS needs the ability to respond to administrative priorities and ensure beneficiaries, providers, and policymakers experience timely, accurate policy execution. Current updates take 7-12 months or longer due to complex coordination between the 3 disparate shared systems and CWF, brittle legacy COBOL code, opaque configurations, and burdensome testing cycles that slow the entire change process.

### 2. Policy flexibility

CMS needs to implement complex or nuanced payment and coverage policies without technical constraint to preserve legislative intent and enable modernized benefit design. The current systems are insufficient for CM's future policy needs.

### 3. Fraud prevention and payment integrity

CMS needs to more consistently prevent and detect fraud and abuse both large and small before payment to protect taxpayer funds and reduce improper payments. Existing legacy architectures rely on nightly batch exchanges and siloed regional data, making rapid detection of bad actors and fraud patterns, real-time risk scoring, and pre-payment intervention challenging.

### 4. Near real-time operations

CMS needs to process and adjudicate claims in near real-time to accomplish CMS payment objectives, support provider revenue certainty, improve beneficiary clarity, and program integrity responsiveness. Nightly batch processing, system latency, and mainframe dependence inherently prevent near real-time adjudication, payment or feedback.

### 5. Program and model scalability

CMS needs to enable new and alternative payment models to operate at national scale to foster innovation and policy testing across the healthcare system. However, current shared systems cannot accommodate modern value-based payment constructs like Innovation models or timely Accountable Care Organization (ACO) reporting, forcing these programs onto separate, duplicative platforms.

### 6. Data accessibility and reporting

CMS needs to provide timely, comprehensive, and accurate reporting and analytics to inform decision-making and policy oversight. The current system is incapable of doing this because data is stored in VSAM files and siloed, non-relational systems that significantly delay and complicate data extraction, correlation, and retrospective analysis.

### 7. Stakeholder visibility

CMS needs to provide beneficiaries, providers, and ACOs with up-to-date claim status and financial transparency to reduce administrative burden and support better clinical and financial decisions. Providers need to be able to upload documents needed to support claims, and beneficiaries need to be able to clearly understand what services were billed on their behalf. Current systems cannot surface near real-time information or out-of-pocket responsibilities.

### 8. Beneficiary clarity and fraud awareness

CMS needs to provide all beneficiaries, but especially those without supplemental coverage, with clear, timely information about their financial responsibility and claim activity in order to prevent financial confusion and enable early detection of potential fraud. Current systems notify beneficiaries only well after claims processing activities occur, which hinders the ability of the beneficiary and his/her representatives to recognize and understand fraud.

### 9. Cost efficiency and system rationalization

CMS needs to consolidate disparate home-grown systems at CMS and the MACs to use taxpayer funds more efficiently and redirect savings toward innovation. At present, multiple auxiliary, stop-gap, and contractor-built tools are required to compensate for shared-system limitations, multiplying cost and complexity, and limiting the availability of funds to be used to innovate payment.

### 10. Policy impact evaluation

CMS needs to quantify, test, back-test, and audit the impacts of policy changes before deployment to improve policy safety, better inform the approval process, and add accountability. In today's legacy environment, the business logic and edits in legacy systems are opaque and scattered, and there is no "model office" environment made to fully test changes and ideas, making impact analysis slow, incomplete, and risky and clearly understand the effect of proposed changes can be challenging.

### 11. Retroactive reprocessing

CMS needs to reprocess and reconcile claims rapidly when policy changes occur retroactively to minimize confusion, interest accrual, and financial risk for CMS and providers. In today's legacy environment, the systems require cumbersome steps to identify, and batch affected claims, and manual, multi-month or even multi-year reprocessing for held or adjusted claims, and are rate limited to 150% of daily claims volume.

### 12. Security and resilience

CMS needs to strengthen cybersecurity and operational continuity across Original Medicare systems to protect beneficiary data, payment integrity, and ensure uninterrupted claims operations. Aging mainframes, unsupported code bases, and limited monitoring capabilities leave the environment vulnerable to breaches, abuse, and downtime.

### 13. Contracting flexibility and innovation

CMS needs to reduce reliance on the shared system maintainers and encourage competitive modernization to lower costs and access innovation from a broader technology ecosystem. Long-standing incumbency and proprietary dependencies constrain competition and inflate sustainment pricing.

### 14. Emergency responsiveness

CMS needs to rapidly deploy system and policy updates during public-health or other emergencies to respond to emerging crises without compromising program integrity or existing non-affected operations. The current legacy systems require lengthy, high-risk change cycles that delay critical updates and heighten fraud exposure.

### 15. Transparency and auditability

CMS needs to ensure that the operational logic, edits, and decision rules within its claims systems are fully transparent and auditable to improve oversight, trust, and accountability. Today's legacy systems obscure business logic, making it difficult for users, auditors, and policymakers to trace decisions or validate outcomes.

#### Opportunities

Re-platforming the shared systems ensures timely, accurate payments, reduces provider burden, prevents fraud, and creates long term savings. ClaimsCore replaces Original Medicare's core systems with a sustainable, policy responsive platform. Further, ClaimsCore implements an underlying preference for Commercial supplies and services to avoid additional costs and schedule (See FAR 12.201).

As a result of project ClaimsCore we expect substantial financial, technical, operational, security and other improvements across CMS, MAC, Beneficiary, and Provider stakeholders.

### CMS-Centric Anticipated Outcomes

- Improved ability to prevent improper payments. Integrating claim level CPI risk scoring enables prepay intervention in real-time subject to applicable policy authority. CPI projects this capability may enable large, recurring reductions in immediate and downstream fraud prevention.
- Usability to support more efficient MAC staff training, streamline workflows and reduce manual processing activities that will decrease operational burden and strengthen long-term organization efficiency.
- Policy agility. Configuration driven rules could allow CMS to implement and test policy changes in hours or days (contingent on process) rather than the current 7-9 month code cycles.
- Enterprise data access. Near real-time reporting and standard APIs increase data visibility for internal stakeholders, providers, and ACOs.
- Single Pane of Glass. One source of truth for Original Medicare's claims processing operations, in a user-friendly and modern UI/system, will reduce the need for custom data flows to support downstream agency operations.
- Improved Zero-Trust–aligned security and resilience. Deployment with 99.9% uptime targets, strong identity, and continuous monitoring improves cybersecurity posture.

- Mainframe risk retirement. Replacing 1970s mainframe/COBOL systems cuts obsolescence risk and dependency on scarce skill sets.
- Faster emergency responsiveness. Configuration-based changes allow rapid policy updates during public health events without waiting for lengthy code releases.
- Nationwide program integrity view. Realtime, cross-region analytics help MACs spot anomalies earlier and coordinate corrective action.

### MAC-centric Anticipated Outcomes

- Usability to support more efficient MAC staff training, streamline workflows and reduce manual processing activities that will decrease operational burden and strengthen long-term organization efficiency.
- Enhanced data access by MACs to relevant data to increase efficiency in Medicare claim process and reduce delays in adjudication
- Coordinated, consistent policy rollout. A single national configuration engine deploys changes consistently across MACs while accommodating MAC and region specific configuration needs, reducing regional divergence and rework.
- Automating test cycles increases system reliability, accelerates release timelines, improves the quality of delivered functionality, reduces defects and operational risk, and decreases MAC manual testing efforts.
- Increased system availability, partly enabled by eliminating batch window constraints, is expected to result in more consistent operational performance, minimized downtime, and to allow MACs to process work more reliably and without interruption.
- Less local middleware and robotic process automation (RPA, e.g. “screen scraping”). Unified APIs and workflows reduce MAC-built workarounds required by limitations in the shared systems today.
- Consolidating IT systems and rationalizing duplicative tools reduces MAC operations and maintenance efforts by streamlining technology footprints, automating manual workflows, and decreasing sustainment overhead resulting in more efficient operations, improved resource utilization, and greater long-term maintainability.
- Standardized edit taxonomy and governance. Configuration over code and transparent rule management reduce idiosyncratic regional behavior.

### Beneficiary and Provider-centric Anticipated Outcomes

- Reduced provider administrative burden in Medicare billing processes.
- Lowered provider burden. Modern APIs, faster decisions, easily accessible documentation submission, and consistent edits reduce administrative waste that today contributes to sizable provider overhead.

- Reduced adjudication time. Claims that previously adjudicated in batches will be adjudicated in near real-time with clear outcomes and claims status which reduce provider follow up, days in accounts receivable, and rework costs while increasing provider confidence in their submissions.
- More predictable cash flow. Faster pay/deny decisions and stronger prepayment controls reduce post-pay recoupments and volatility.
- Fewer resubmissions. Immediate, precise edit feedback lower avoidable improperly submitted claims and resubmits.
- Accurate patient responsibility estimates. Near real-time adjudication supports point of care cost clarity and fewer financial surprises for patients, especially the ~10% of beneficiaries without supplemental coverage.
- Faster retroactive corrections. Automated, high-volume reprocessing of retroactive policy changes reduces confusion, interest accrual, and manual fixes.
- Clearer appeals and medical review. A full rule/explanation trace per claim streamlines documentation for reconsideration and audit.
- Earlier fraud/identity issue detection. Real-time cross-checks and beneficiary visibility help surface suspect activity before it becomes a denial cycle.
- Consistency for multistate systems. Multistate health systems report multiple unexpected variations MAC to MAC. ClaimsCore will introduce improved consistency in interstate experience with CMS systems reducing provider burden and frustration while still respecting local coverage determinations.

## Approach

### Assumptions

1. Software Vendor: CMS intends to procure a SaaS based COTS platform, through a competitive process, to be configured and extended by the vendor in collaboration with CMS, MACs, and/or supporting contractors.
2. Professional Services: CMS envisions its primary role as policy development and oversight and expects to contract for operational services either as part of the software offering in a traditional SaaS model or with a software vendor and systems integrator team depending on the relationship of the services component to the software vendor.
3. Scale assumptions: ~1.2 billion claims per year (for sizing) and ~33.6 million beneficiaries in Original Medicare. CMS prefers a single scalable instance of vendor software supporting all beneficiaries; however, load may be distributed across an instance per MAC or MAC region if analytics, editing, and real-time program integrity have real-time cross-region awareness.

4. Stakeholder engagement: The contractor(s) are expected to coordinate closely with CMS, MACs, and Providers in workgroups, demos, requirements gathering and validation, training, and communications facilitated by the vendor and contractors in partnership with CMS.
5. Incremental delivery: Phased deployments including incremental run-out based roll outs including focused workstreams with defined scope, resources and timelines. Vendor as well as independent validation of outputs compared against legacy systems running in parallel will provide objective evidence of parity and reduce risk.
6. Warranty and Service Level Agreements: Contractor(s) must ensure appropriate system performance based on operational needs assessment and tied to payment penalties.

### Cost Drivers

1. Beneficiaries & claim volume: As noted in the assumptions.
2. Rule complexity & change frequency: Thousands of edits and frequent updates; extensive regression and validation required.
3. Integration points: Numerous external systems (e.g., PECOS for provider enrollment, Pricers, Fee Schedules, Coding, Beneficiary Eligibility, etc.); HIPAA X12, FHIR, REST APIs with complex mapping and maintenance.
4. Data migration & history: Decades of VSAM and flat-file data, messy provider and beneficiary data, and the extraction, cleaning, and transformation needed to make this data usable.
5. Business Logic migration: Extensive COBOL code logic with little documentation needs to be analyzed and the relevant logic imported into to the new system. CMS is undertaking experimental efforts to extract and provide business logic and edits to awardees, but Contractor(s) are ultimately responsible for fully and correctly migrating business logic, in order to achieve parity with the outcomes of the existing systems.
6. Testing & validation: Large-scale regression, performance, and parallel runs where differences in outcomes must be explainable.
7. Availability & resilience: 99.9% uptime target with redundancy, DR, failover, monitoring, and surge capacity needed.
8. Stakeholder engagement & training: Stakeholders include CMS, MACs, providers, and clearinghouses. Each will require collaboration, training, documentation, and change management.
9. Regulatory & compliance: HIPAA, FISMA Moderate, CMS ARS, Section 508; controls, audits, documentation, and certifications.

## Requirements

The following list represents a consolidated list of requirements focused largely on technical and operational items that are high priorities for CMS. In addition, further requirements are set forth in the sections that follow (e.g. Proof of Concept Scope, Production Implementation).

1. System Performance & Operational Efficiency: CMS requires a system that adjudicates claims accurately in near real-time, is easy to configure, is extensible, supports CMS/MAC strategic objectives, people, process, policy, and technology, and improves operational efficiencies. A target of 99.9% uptime, horizontal scalability, and zero/minimal downtime releases are required. Additional objectives are listed in the POC Metrics and QASP.

2. Architecture & standards: The solution must align with CMS enterprise architecture and standards including but not limited to those set forth in Appendix E: General CMS & Related Technical Standards. Contractors should plan to work with CMS Enterprise Architects to ensure they aren't duplicating existing functionality or creating unnecessary duplicate tooling and are leveraging existing tools where appropriate. CMS anticipates each vendors' solution may be unique in the way a shared responsibility matrix is completed, however, as a general principle, vendors should expect to operate, configure, manage, and control their own systems with CMS providing oversight, requirements, and guidance.

3. SaaS Deployment Models: CMS is interested in receiving proposals from vendors offering either a fully managed Software as a Service (SaaS) deployment hosted in a vendor-owned cloud or a vendor-managed SaaS deployment hosted within a CMS cloud infrastructure, which will be furnished by the Government. Contractors may choose to provide information for one or both deployment models if either can be supported and how each may affect cost, timeline, information security requirements, and other relevant differences. Note there are material additional FISMA Moderate ATO and FedRAMP related requirements when deploying in a vendor cloud environment which may not apply to CMS cloud infrastructure. See Requirement 4: Security and Privacy for more information on the required Authority to Operate for each of these models.

4. Security & privacy: Vendor must satisfy all CMS cybersecurity requirements including security frameworks, compliance, oversight, incident reporting, personnel security, and data handling. See Appendix A: Security Requirements for additional details. Key security priorities include:

    4.1. ClaimsCore will be considered a FISMA Moderate system, and/or FEDRAMP SaaS will be required for all solutions. Vendors will be required to implement the controls listed in the CMS Acceptable Risk Safeguards (ARS) at the Moderate baseline at a minimum (353 controls). Controls can be found at https://www.cms.gov/files/document/acceptable-risk-safeguards-v51.xlsx

        4.1.1. For solutions deployed in a vendor-owned cloud environment or as self-hosted SaaS in a datacenter, CMS will support the vendor in procuring an ATO and sponsor a FEDRAMP certification, if needed. The vendor will be required to produce all

necessary documentation and auditing required to prove compliance for all controls.

4.1.2. For solutions deployed in the CMS Hybrid Cloud, CMS anticipates leveraging its existing FISMA Moderate ATO environment for control inheritance. Use of the CMS cloud allows vendors to fully inherit 83 controls and partially inherit another 236 controls.

4.2. The vendor must ensure full compliance with all mandatory annual audits: Cybersecurity and Risk Assessment Program (CSRAP), System Census, CFO Audit, A-123 Management Controls Audit, HHS Appendix IX Financial Audit, and Major IT Business Case (MITBC) Financial Review. The vendor shall provide timely support for ad hoc audits including Office of Inspector General (OIG) audits and OIT data calls. The vendor is responsible for annual review and maintenance of Authorization to Operate (ATO) supporting documentation, security control assessments, and timely reauthorization submissions. The contractor shall maintain operational responsibility for their assigned CFACTS database instance in accordance with CMS standards. All audit requirements must be satisfied within established timeframes with complete documentation maintained per federal records management requirements and CMS policy directives. See https://security.cms.gov for security and privacy policy and standards in place for CMS information systems.

4.3. Vendors should propose their information security framework, secure development lifecycle (SDL) practices, threat modeling, and security testing, and risk-based vulnerability management in the PWS and provide a copy of their shared responsibility matrix including all relevant parties.

4.4. The vendor should expect employees with access to CMS systems, facilities or data will be subject to standard CMS vetting procedures, with additional screening for foreign nationals. All work must be performed in CONUS and non-public data may not leave CONUS.

4.5. Vendors should plan to submit documentation on existing certifications, controls, and compliance frameworks that have been achieved and implemented such as HITRUST R2, SOC II Type II, FEDRAMP, ISO/IEC 27001, NIST CSF, etc. Certification boundaries for specific software or systems should be clearly stated.

4.6. Vendors should plan to use CMS Identity Management (OKTA) for authentication (not authorization) to their platforms. All users accessing the product, CMS data, CMS information, or CMS information systems under this contract must complete the required Vetting and Credentialing (V&C) process prior to being granted any form of logical or physical access.

Vendors should plan to, at contract award, submit to the Contracting Officer (CO) and/or Contracting Officer's Representative (COR) a complete roster of all relevant personnel. Each individual on the roster will receive an invitation from the CMS ICT website to register an account and begin the V&C process. Failure to submit a roster on contract

award or of employees to fill out the registration in a timely manner will materially delay the start of work. Details on registration can be found here https://www.cms.gov/About-CMS/Contracting-With-CMS/ContractingGeneralInformation/Downloads/PolicyandGuidance/EFI-New-User-Guide-v28.pdf

5. Data Rights: To avoid vendor lock-in while honoring commercial-item norms, CMS requires the following rights framework for data, software, and technical artifacts generated under this effort.

   5.1. CMS data and derived data. CMS retains ownership and unlimited rights in all CMS data handled or produced under the contract, including derived data, logs, metrics, audit trails, telemetry, claims data, claims history, data loaded from external CMS systems, adjudication related outputs, and decision explanations. Contractor shall not assert any license over CMS data.

   5.2. Custom code and technical artifacts. Contractors should use configuration of their systems where possible over custom code to avoid breaking upgrade paths and introducing additional testing burden. For any software, scripts, transforms, connectors, interface shims, test harnesses, schemas, specifications, runbooks, training, and documentation first produced under this contract and not constituting Commercial Computer Software, CMS receives unlimited rights; source form must be delivered.

   5.3. Rules, edits, and configurations. Vendor will supply on request vendor-neutral representations (e.g., spreadsheets/CSV/JSON/YAML, prose rulebooks, diagrams, API/interface specs) which shall be delivered with unlimited rights so they can be published, competed, or re-implemented without restriction. Platform-specific representations (e.g., exports in the product's Domain Specific Language (DSL), proprietary rule/config bundles) shall be provided with perpetual, irrevocable, paid-up, government-purpose license rights allowing use, reproduction, modification, and disclosure within CMS, MACs, and CMS-directed support contractors for any Government purpose (operations, validation, transition, recompete, etc.), but not for commercial resale. Contractor shall also provide timely, complete non-proprietary exports sufficient to reconstitute equivalent behavior on another platform.

   5.4. Adapters, connectors, and integration assets. Assets first produced under this contract shall be delivered in source form with unlimited rights. If an asset necessarily embeds contractor background IP, CMS shall receive government-purpose license rights to the embedded portions and unlimited rights to all CMS-specific logic, mappings, and interface specifications surrounding them. Contractor shall establish and maintain accessible repositories of interface specifications and supporting documentation in machine-readable format that enable third-party integration without original equipment manufacturer coordination.

   5.5. COTS and contractor background IP. CMS does not seek ownership of the contractor's proprietary platform or background IP. CMS will accept the standard commercial license

to operate the platform, provided the license permits operation by CMS, MACs, and CMS-directed support contractors, supports non-prod, DR, and performance testing use, does not impede data/config export or portability drills, and includes reasonable termination assistance/step-in to protect continuity. CMS claims no ownership to vendor proprietary code, trade secrets, etc. and expects to acquire only those rights customarily provided for commercial computer software.

6. Interoperability: The solution must support HIPAA X12 and comprehensive APIs (REST/FHIR, events), avoid creating new data silos, and support for CMS-0057-F.

7. Legal and HIPAA Requirements: The vendor shall comply with HIPAA, the HITECH Act, and all applicable federal privacy and security regulations (45 CFR Parts 160 and 164). The vendor shall protect all PHI and PII in accordance with CMS privacy and security policies, maintain a valid Business Associate Agreement (BAA), and ensure all data use and disclosure are authorized, logged, and limited to the minimum necessary. One or more data use agreements (DUA) will be required.

8. Audit & transparency: The proposed solution must support full edit and rule explanation trace, decision logs, audit logs, and change history to meet CMS transparency objectives.

9. CMS & MAC Operations: The Contractor should expect to support CMS and MAC workloads, operations, business processes, policies, systems, and other needs without expectation of policy change to accommodate the contractors' existing suite of products. CMS may elect to adjust process, policy, or other practices at its discretion based on capabilities offered by the proposed product suite.

10. Specialty Workloads: CMS and MACs support certain specialty workloads and processes outside of the standard MAC jurisdictions. They include but are not limited to claims processing for Railroad Board beneficiaries, the Mass Immunizer program, limited Indian Health Services support, Qualified Chain Provider/Out of Jurisdiction Provider support, Histocompatibility Labs, and the electronic Medicare Equivalent Remittance (eMRA) workload for the Veteran's Health Administration. Additional workloads that may or may not require claims processing can be found in Appendix G: Specialty Workloads

11. Historical Data: The solution must support use cases for the administration of historical data including importing or retrieving historical data from external archive sources and subsequently analyze, report on, reprocess, and/or make mass adjustments. Additionally, the ClaimsCore system must synchronize its own unique claims history with that of the legacy system on an ongoing basis during the transition to full production for all MAC jurisdictions.

12. No disruption: Incremental delivery and parallel operations to maintain current processing throughout migration. The CMS proposed cut over strategy is described in more detail in "MAC Onboarding".

13. Export and Transition: CMS values and is prioritizing its ability to transition to a new provider of claims adjudication software for any reason. Accordingly, CMS requires:

13.1. **Portability:** Vendor must provide documented export formats & APIs and support no-fee bulk export during transition or step-in and portability dry-runs.

13.2. **Escrow/termination assistance:** updated runbooks, custom code, config snapshots, and data-model documentation, training, and all other relevant assets placed in escrow; termination assistance CLIN with defined SLAs.

13.3. **Vendor Shutdown**: CMS will receive transition assistance and step-in rights to continue operations on the contracted platform and will receive all configuration/data exports necessary to transition. Further, CMS must have the unrestricted rights to export, transition, or operate the system independently in the event of vendor termination, acquisition, change of control, or failure. Step-in and independent operation must be technically enabled through Government controlled tenant administrative accounts and Government controlled enterprise IdP. CMS shall be able to administer access/roles, system configuration, and audit logs, and execute data/configuration export without contractor assistance during dispute, termination, shutdown or change of control.

13.4. **Standards:** The solution must be built on open, standards-based architecture with full data portability. Proprietary components must not restrict interoperability or create undue switching costs.

### Professional Services

CMS will require professional services to configure, implement, integrate, secure, operate, validate, and transition to the selected COTS platform within the CMS and MAC environments while ensuring continuity of operations for all stakeholders including certain provider users. The contractor's professional services are expected to include the services listed below and may include others as additional needs are discovered.

1. **Product & Project management and integrated planning**: In partnership with CMS and MACs, develop and continuously maintain a comprehensive, end-to-end implementation plan covering discovery through transition. At a minimum, include an Integrated Master Plan/Schedule (IMPS); work breakdown structure (WBS) with named work streams; a risk/issue/assumption/decision (RAID) register with mitigation owners; stakeholder engagement / user research & feedback / communications plan; compliance checklists (CMS ARS/FISMA, HIPAA, Section 508, TIC 3.0); Responsible, Accountable, Consulted, and Informed (RACI) matrices; environment/cutover runbooks; defect and change logs; test and validation strategies (including dual run parity metrics, performance/DR drills, and acceptance criteria); training and knowledge transfer materials; and measurable milestones used for inspection/acceptance and QASP reporting.
2. **Integrate with upstream and downstream systems using open standards.** Build, test, and certify required interfaces (e.g., HIPAA X12, REST/FHIR, events, batch bridges as needed) with CMS, MAC, provider, and partner systems. Interfaces must be based on industry standards and avoid proprietary protocols or formats and include clear, comprehensive

documentation. The legacy Shared Systems and CWF have hundreds of individual interfaces (file exchanges, API calls, X12 transactions etc.) that enable critical business processes both as part of the claims adjudication process and downstream that must continue to function as expected. Examples include systems hosted by CMS and MACs such as HIGLAS, PECOS, BIC, Pricers/Groupers, Customer Service Interfaces, Documentation and Reporting, Banking, Document Management, Printing Services, etc.

3. Extract and document business rules. Elicit, extract, normalize, and document legacy rules/edits and hard coded business logic in a vendor neutral format (e.g., spreadsheets/JSON/YAML + prose rulebook), establish traceability to policy, and provide explainability for adjudication outcomes. CMS has undertaken significant efforts to extract this information prior to the start of the Proof of Concept, but additional work is likely to be needed.

4. Plan and execute data migration. Design and perform ETL (history and in-flight), mapping, data quality controls, reconciliation, and lineage documentation appropriate to the adjudication strategy employed by the vendor system.

5. Support dual run testing and validation. Stand up parity/variance harnesses, test oracles, and dashboards to measure adjudication outcomes relative to the legacy system. Vendors should meet success metrics (e.g., outcome match rate and dollar variance thresholds), provide root cause analysis for differences, and drive remediation to closure.

6. Training and learning management. Provide role-based training for CMS and MAC staff; develop and maintain Learning Management System (LMS) curricula, produce job aids and quick reference guides, deliver train the trainer sessions, and demo/sandbox environments

7. Change management and stakeholder communications. Coordinate with MACs and affected CMS components to minimize operational impact. Contractors should plan to conduct discovery, document CMSMAC processes and job roles that will be impacted by replacing the Shared Systems and CWF. Contractors should coordinate CMS/MAC communications and training (webinars, notices, team meetings), publish and execute cutover playbooks and manage issue communications during dual run. Once the vendor solution has been moved into a production capacity, vendors should expect to work though CMS change control processes.

8. Operations readiness and cutover. Contractor should manage a run out based migration on a MAC by MAC or region by region basis, deliver runbooks, SRE/on call procedures, performance tuning, DR playbooks, and acceptance criteria for go live. In addition, the contractor should ensure all upstream and downstream integrations are certified and functioning properly.

9. Performance, cost, and reliability engineering. Ensure the system meets SLOs for latency, throughput, and uptime. Provide instrument dashboards, right-size cloud resources and optimize consumption per CMS guidelines.

10. Accessibility and documentation. Maintain current system diagrams, interface catalogs, data dictionaries, runbooks, and user guides and ensure all deliverables (documents, training, dashboards) meet Section 508/WCAG conformance.

11. Reporting and analytics enablement. Understand CMS/MAC reporting needs and implement required reports/exports using product capabilities. Expose and support implementations accessing APIs and documented schemas to support CMS and MAC analytics.

12. Portability drills and exit readiness. Perform end to end export and rebuild exercises to a clean CMS tenant or export depending on the deployment architecture (data + configurations + rules + integration assets), fix gaps, and deliver reports. Ensure artifacts are provided in documented, machine readable, vendor neutral formats.

13. Post-go-live stabilization and optimization (hypercare). For each cutover (by MAC, region, and/or claim family), provide an initial hypercare period to stabilize operations. Monitor and meet all QASP SLOs (uptime, latency, variance/defects), operate 24×7 incident, problem, and change management. Complete one DR failover/failback exercise with after action report. Tune performance and cloud consumption. Continue dual run variance monitoring where applicable and drive root cause remediation. Execute continuous monitoring obligations for ATO (SSP/SAP/SAR, POA&M updates, vulnerability remediation within CMS timelines). Refresh runbooks and O&M procedures. Deliver ongoing role-based training and knowledge transfer to CMS/MAC operations. Publish live dashboards and a post implementation report to the COR.

14. Professional services availability. Provide scalable professional services capacity (including surge) throughout the life of the contract to support ongoing change requests, implementation, operations, variance remediation, security updates, and transition activities.

### Governance, Engagement & Communication

CMS plans to establish a tiered governance model that is highly responsive to day to day needs of implementers, MACs, and other stakeholders. CMS has identified key risks, long lead activities required to implement a new claims administration system, and other potential points of friction, however we are also planning for a significant number of unknown variables and challenges that require a responsive group of decision makers and operators to drive issues to resolution. CMS plans to proceed iteratively, this structure is subject to change based on current needs.

1. Executive governance board: CMS leadership and key stakeholders set enterprise direction, approve cross-MAC sequencing decisions, approve policy and process change, and resolve escalations and tradeoffs that require leadership input.

2. CMS Workgroup: An empowered group of CMS stakeholders working with vendors will provide direction, oversight, manage change, and recommend sequencing based on MAC resources, readiness, operational risk, and statutory/regulatory timelines.

3. MAC and CMS SME Workgroups: When vendors or contractors have questions regarding policy, process or technology SME workgroups will be available to help answer questions and guide any regulatory, policy, or operational change that may need to be proposed.

4. Tiger teams: Time-boxed tiger teams are formed as needed to drive issue-specific execution to closure (for example, integrations, operational readiness, and validation), and to rapidly surface decisions and impacts to the CMS workgroup and governance board.

### Collaboration Tools

ClaimsCore contractors must engage with relevant CMS workgroups, offices, MACs, and partners through regular demos, open documentation, targeted training, standups, and efficient asynchronous updates (email, slack, Jira, etc.). Educational materials and hands on sandboxes should be provided to help build consensus on process especially where policy changes may be needed.

The tools referenced below are the CMS managed instances and will be furnished by CMS for the Contractor's use where relevant.

- Slack:
    - Primary communication method
    - Shared channels for cross-team topics
- Confluence: All documentation will be stored here, including roadmaps, decision log, assumptions, meeting agendas and notes, research artifacts, team contact information, tech specs, etc.
- JIRA: Teams will utilize JIRA dashboard and reporting capabilities.
- GitHub: Single, open-source code repository. Contractors should expect to commit custom code developed for the government in a government owned GitHub. Where relevant, GitHub pull requests should be linked to JIRA user stories to connect the change to the requirements addressed.

### Reporting

The Contractor should maintain clear government visibility into program cost, schedule, progress, technical issues, performance, and risk, including periodic reporting. The Contractor should deliver meaningful reporting and analytics that provide the Contracting Officer's Representative (COR) and Product Manager(s) with up-to-date and comprehensive information regarding technical and management performance. Whenever possible, the Contractor should reference and/or populate all status reporting with live data, from live dashboards, when available and practicable. Live data dashboards should be sourced from the Agile tools under this contract, or other resources as directed by the COR.

Monthly Status Reports will be reviewed with the Contracting Officer (CO), COR and the Contractor's Program Management team. The Contractor should report the status of the following:

- Status of and progress towards all items on the Integrated Master Plan & Schedule (IMPS)
- Accomplishments
- Deliverables (including data delivered to CMS)
- Risks
- Self-assessment of performance against metrics from QASP
- Management information including financials (invoices submitted or approved, estimate at completion, etc.) and other productivity data (e.g., velocity, burn down chart, burn up chart, etc.)
- Personnel roster (including the job title, labor category, vacancies, and name of the prime or subcontractor employing the person/position)
- Project Status Dashboard should be periodically reviewed with the COR, Product Owner and the Contractor's Project and Operational Management teams. It should also provide an overview of all projects and operations with a focus on outstanding issues and risks.

## Challenge-Based Acquisition

ClaimsCore will be procured through a multi-phase challenge process. The objective is to create an environment where acquisition decisions are based on experimentation and demonstration of existing or emerging technology through a rapid and impactful assessment of commercial solutions and competing "prototypes" (i.e., limited implementations).

CMS contemplates multiple awards including a few contracts – perhaps as many as four or perhaps only one. Due to the operational cost and burden of a PoC, fewer awards are preferred. **Accordingly, CMS has established an aggressive base-period (POC Phase) affordability objective. CMS encourages bidders to propose the best Proof of Concept solution possible at the lowest possible cost.** Those vendors will begin work under a proof-of-concept (POC) phase where their solutions are tested against real CMS data and measured against CMS-established success criteria and metrics.

After the POC phase, CMS anticipates the down-select of contractors by not exercising option(s) for further work based on unilateral determination of CMS' best interest. This approach ensures solutions are validated in practice, stakeholder confidence is built incrementally, and only Contractors with proven capability at scale advance. Contractor solutions will be assessed against the success criteria, and CMS anticipates, but does not guarantee that a Contractor will be selected, via option exercise, for an eventual production implementation to replace the Shared

Systems and Common Working File and integrate with associated systems and business processes (e.g., CMS change management, MAC business operations, etc.).

### Proof of Concept Scope

During the challenge, contractor solutions will be run in parallel with CMS's legacy shared systems. This head-to-head approach ensures that performance, accuracy, and reliability can be directly measured against current operations. Contractors must demonstrate that their platforms can adjudicate Part A, Part B and DME claims in near real-time, deliver outputs consistent with legacy results, and provide transparent explanations for any variances. Success will be evaluated based on clear, measurable metrics defined in the POC Metrics table and QASP including accuracy, throughput, interoperability, and stakeholder satisfaction. CMS anticipates that only one solution will advance to production.

### MAC Related Scope

Only MCS, FISS, DME, and CWF are in scope for this replacement. No MAC owned and operated systems are expected to be modernized during this implementation at this time but may be considered in future procurement actions. CMS expects the ClaimsCore solution to support the full scope of MAC operational responsibilities that are currently enabled by MCS, FISS, DME, and CWF, while maintaining uninterrupted Original Medicare operations during transition. To limit scope and reduce risk, CMS prefers contractors support integrations with existing MAC tools and systems rather than replacements, though in certain exceptional circumstances a replacement could be considered. CMS expects continuity of the business outcomes and controls across the end-to-end claim lifecycle, including intake, eligibility and coverage checks, edits and rules execution, payment determination, remittance and beneficiary notice generation, adjustments and reprocessing, reporting, auditability/traceability and other relevant MAC responsibilities.

Offerors should assume the solution must also support, either natively or through integration, the downstream and operational functions required for CMS and MAC performance, including customer service and inquiry support, MSP and coordination of benefits, benefits coordination and recovery, medical review and related documentation workflows, appeals and audit support, print and mail outputs, testing and validation, banking and payment operations, accounts receivable review, and CMS reporting. Only a subset of all required functionality will be implemented during the proof of concept.

Offerors may consider the documents linked in Appendix F: MAC Statements of Work and the MAC Workload Transition Handbook as a reference for the breadth of MAC responsibilities. CMS anticipates refining process details during discovery and implementation planning, and expects phased deployment with MAC participation, training, and change management, with validation against legacy outputs during parallel operations as needed to ensure continuity.

MACs, by design, have the authority to implement local coverage determinations, edits, and certain policies autonomously. CMS is not changing its policy regarding that structure. CMS will continue to set national coverage determinations, policies, and edits. Contractor software must

support MACs ability to implement local coverage determinations where national coverage determinations have not been specified by CMS.

### Fraud Prevention System

CMS is not seeking to replace its existing Fraud Prevention System at this time, however, it is interested in evaluating vendor systems' abilities to integrate with the existing FPS at CMS, facilitate rapid changes to program integrity related edits, support claim-level risk scoring, support for pre-payment program integrity controls, analysis tools that help stakeholders understand the impact of proposed changes quickly or help measure and monitor the impact of an implemented change, and integrate with new program integrity tools in the future.

### Deliverables

For the POC, each contractor will be responsible for planning and driving the work needed to meet the challenge success criteria, including organizing working sessions and demos, arranging and documenting discovery with CMS and MAC stakeholders, managing their implementation schedules and milestones, coordinating dependencies and data needs, and running their own analysis, configuration, testing, and defect resolution activities within the PoC timeline. CMS will provide environments, data, and points of contact, but contractors are expected to proactively manage and coordinate all work necessary to demonstrate their solution's capabilities.

During the PoC phase, CMS expects the contractor to demonstrate a production-like, end-to-end capability sufficient to evaluate the metrics laid out later in this section along with feasibility, performance, security posture, and operational fit, and to build confidence with CMS and MAC stakeholders that the solution and team can support Original Medicare scale and complexity. PoC scope may include, but is not limited to:

1. Adjudicating large claim volumes quickly and accurately. Accuracy will be measured through both CMS and contractor tools that compare adjudication outcomes and artifacts with the legacy system. For example, the Electronic Remittance Advice (ERA) from both systems may be used to verify payment accuracy and other data.
2. Successfully integrating with Tier 1 Systems as described below.
3. Demonstrating user interfaces and operational workflows (including both end-user and administrative functions) relevant to the PoC claim scope including any pre-configured Original Medicare rule sets, workflows, or configuration.
4. Configuring and demonstrating flexibility and speed in adding or updating edits, workflows, integrations, business rules, reference data, and related configuration artifacts needed to achieve target performance, accuracy, and variance metrics.
5. Demonstrating security compliance and an ATO-ready posture appropriate to the PoC environment, including required controls, logging, access management, and vulnerability remediation practices.

6. Performing load and performance testing at CMS-specified volumes and profiles, and providing results, bottlenecks, and remediation plans.
7. Demonstrating responsiveness to CMS and MAC stakeholder feedback, including timely issue triage, defect resolution, and change incorporation within the PoC timeline.
8. Building confidence through transparent reporting of progress, risks, dependencies, and objective performance results against CMS-defined metrics.
9. Delivering PoC artifacts such as interface specifications, configuration documentation, test results, variance analyses, and an Integrated Master Plan & Schedule (IMPS).
10. Develop a CMS-reviewable production IMPS that defines the target operating model, documents impacted people, processes, and systems, identifies and quantifies required changes and operational impacts, and presents a phased, CMS-approved path from proof of concept to sustainable production operations.

### Dependencies and Integrations

During the proof-of-concept phase, CMS expects contractors to integrate with the external systems and data sources identified in Appendix D, Tier 1 Systems List. These systems are essential to the adjudication of most Original Medicare claims. CMS will ensure that the relevant systems are available for integration or that required data, specifications, and connectivity are made available to awardees for ingestion, as appropriate. Vendors may be required to transform or adapt provided data to align with their solution's data models and schemas. CMS will provide available interface documentation for each integration; however, contractors should anticipate that additional discovery and clarification may be required during implementation. While the Tier 1 Systems List may be refined as additional information becomes available, it should be considered directionally accurate for purposes of planning and execution.

Contractors should not assume that inbound transactions have been fully validated for completeness, internal consistency, or semantic correctness prior to reaching the contractor system boundary, and should plan to perform any additional validations (e.g. SNIP Level 5) necessary to safely process claims.

To assist contractors in adjudicating claims, CMS will provide the following:

- Rule and logic artifacts: Legacy business-rule extracts (COBOL/ALC/HLASM code, code analysis, and configuration repositories), edit taxonomies, pricer/ grouper specifications, fee schedules, and reference documentation for at least one MAC jurisdiction. Contractors should expect these may be incomplete and require additional discovery.
- Data sets and connectivity: Connectivity to data streams, external systems, and information sources which may include, but are not limited to, APIs, S3 buckets, SFTP, Redshift, Kafka, and other CMS-approved protocols. CMS will provide test claims, adjudication outcomes from legacy systems for test claims, eligibility/benefit context, and

test endpoints for appropriate Tier 1 external systems. This will include, but is not limited to:

  - Beneficiary/member data for the ~33.6M Medicare beneficiaries.
  - Provider data (enrollment, etc.) for all Medicare providers.
  - Up to 3 years of historical claims data for Medicare Part A and B claims, for at least one and possibly all MACs.
  - A claims test set along with the adjudicated claim and any available outputs such as the Electronic Remittance Advice

- Points of contact and workgroups: CMS and, as appropriate, MAC personnel to work with for discovery, clarifications, data/interface questions, and issue resolution on a defined cadence during the PoC.

### POC Assessment Metrics

The table below sets out representative assessment criteria and measurable objectives for the POC. These objectives reflect CMS's view of high-quality performance, however, proposals and eventual awardees will be evaluated relative to one another and to industry standards as evidenced in the submissions (CMS may calibrate thresholds based on the distribution of demonstrated capabilities). CMS may refine thresholds, weights, or add/remove criteria where in the Government's best interest. Contractors will be assessed on their ability to meet or exceed these objectives, along with qualitative considerations such as risk, feasibility, and commercial terms. CMS reserves the right to validate claimed results and require supporting evidence. During the PoC, contractors will configure their systems, gather requirements, and integrate with external systems before the start of the Measurement Interval. The Measurement Interval will be a defined window near the end of the Base Period during which CMS and contractors will formally measure performance against the criteria in the table below.

These metrics are intended to be a standardized baseline for evaluating parallel processing and dual-run success criteria. MAC-specific variations may be proposed based on specific needs, but CMS will evaluate and approve deviations from the baseline case by case through governance.

| Metric | Objective |
|---|---|
| Availability, responsiveness & escalation | 24×7×365 support; P1 response ≤30 min, P1 service restoration ≤4 hrs.; named Technical Account Team; on-call SRE coverage |
| Median deviation of dollar value on paid claims (dual run) | Median <0.5% and p95 ≤1.0% variance vs. legacy; 100% explainability of differences, with a root-cause report within 10 business days for all differences. |
| Alignment with legacy outcomes (claim match rate) | ≥95% of claims produce the same outcome state (e.g. pay, deny, suspend); 100% explainability of differences, with a root-cause report within 10 business days for all differences. |

| | |
|---|---|
| Historical data migrated or accessible | 100% of designated claims history cleaned, mapped, and migrated or virtualized; reconciliation error rate ≤0.2% of records; data lineage documented. |
| Legacy rules extracted and implemented | ≥95% parity by regression tests across the top 95% of claim volume; remaining deltas documented with mitigation plan. |
| Live interfaces with external systems | Total number of interfaces to external systems fully implemented in the evaluation period |
| Training and consensus-building | Delivered to all relevant stakeholders evaluating PoC; >70% satisfaction rating; publish role-based cheat sheets. |
| Throughput, latency, uptime, scalability | Uptime ≥99.9% monthly; p95 ≤1s, p99 ≤2s adjudication for clean claims (measured within vendor boundary); sustain ≥4M claims/day and burst to 2× within 15 minutes without manual intervention. |
| Implementation of new payment models | Configure and demo ≥1 alternative payment model without code changes; time-to-configure ≤30 days from approved spec; provide what-if impact and near-real-time metrics (<24 hrs.). |
| Cross-MAC data unification & analytics | Demonstrate incoming claims are adjudicated using claims data across all MACs and jurisdictions (no regional or contractor-specific data silos) and that near real-time cross-MAC business intelligence views are available. |
| Pre-implementation planning | Deliver an integrated master plan and schedule (IMPS) to parity and production ≤36 months, with critical path, dependencies, staffing, stage-gates, and risk register. |
| Reduction in administrative costs | Present a cost-to-serve model with assumptions; target ≥10% reduction in CMS/MAC admin costs within 36 months of go-live; identify measurement method. |
| Demonstrated support for rapid policy change support | Policy change cycle time ≤15 business days from approved spec to production; what-if analysis outputs within 48 hours; provide provider audit reports/dashboards. |
| Broadly positive stakeholder feedback | CMS/MAC CSAT ≥85% during pilots. |
| Satisfies all CMS security and compliance requirements. Zero security incidents. | Meets CMS ARS; FedRAMP Moderate (as applicable) or ATO path; no open Critical/High vulns at go-live; POA&M: 0 Critical/High past due; patching: High/Critical ≤30 days. Shared responsibility matrix completed and accepted by CMS. |
| Commercial terms acceptance | Contract modification during PoC to more specifically address option-year gating tied to outcomes; price-escalator caps & benchmarking; portability & step-in rights; audit rights and other relevant contract terms. |

| | |
|---|---|
| Total cost of ownership | Provide 5-year net present cost and unit pricing. Include price-cap and true-up/true-down terms. |
| Established policies, procedures, and implementation of backup and DR plans | RTO ≤4 hrs., RPO ≤15 min; annual DR test pass with report; failover/failback time documented |
| Features and Functionality | Contractors will complete a capability matrix based on the features and functionality listed in Appendix C. Contractors may include additional features in their matrix that are not represented in Appendix C. |

### Integrated Master Plan & Schedule (IMPS)

After POC contracts are awarded, CMS anticipates approximately 1 month of contractor onboarding activity that includes required contractor vetting prior to accessing CMS environments and data. Contractors should expect to use that time to collect information and plan their implementation. The Contractor shall submit a PoC IMPS to CMS within 10 business days of the PoC kickoff (or other date specified by CMS at award). The Contractor shall update and resubmit the IMPS within 5 business days of receiving CMS feedback until CMS approves the baseline IMPS in writing.

CMS encourages Contractors to use planning strategies, materials, and cadences that have worked best for them in prior implementations; however, the IMPS shall be a single, integrated plan and schedule that is sufficient for CMS to track progress, assess feasibility, and compare performance to stated PoC deliverables and metrics. At a minimum, the IMPS shall include:

1. A Work Breakdown Structure (WBS) aligned to PoC Deliverables and the PoC Assessment Metrics, with objective acceptance criteria and required evidence for each WBS element.
2. A milestone schedule through the end of the PoC including critical path, milestone dates, dependencies (including CMS-furnished access, data, and Tier 1 system connectivity, etc.), planned demonstrations and reviews, and the milestone acceptance criteria.
3. Planned checkpoint dates for each applicable PoC Assessment Metric, including “Pre-implementation planning” (integrated plan to parity and production).

Frequent contractor updates (e.g. weekly scrum, or cycle meeting) shall include progress against milestones, schedule variance versus the approved baseline, forecasted completion dates, and blockers requiring CMS action. The Contractor shall not change the baseline milestone dates or scope without CMS approval. Any requested change shall include the rationale and impacts.

CMS’s objective is an efficient and comparable evaluation of PoC participants. CMS may discontinue a Contractor’s participation in the PoC if the Contractor:

1. Misses a critical milestone without a CMS-approved recovery plan.

2. Fails to demonstrate measurable progress against agreed milestone dates for PoC Assessment Metrics.
3. Fails to provide required IMPS updates or required milestone evidence.
4. Otherwise demonstrates an inability to complete the PoC scope within the PoC period.

During the POC, Contractors should begin preparing a proposed Production IMPS to satisfy the additional requirements of a production implementation. The plan must document current-state people, process, and technology dependencies that would be impacted by production deployment. It must identify the people, process, and technology changes required to operate the solution at scale, including training needs, staffing model adjustments, workflow changes, and opportunities for system rationalization. Any proposed deviations from current CMS or MAC operating models must be clearly identified, justified based on measurable efficiency, cost, or sustainability benefits, and submitted for CMS approval. The plan must also include a phased rollout and transition approach suitable for CMS approval and aligned to proof-of-concept results and production readiness criteria.

## Production Implementation

The contractor, in partnership with CMS and MAC personnel, will execute an incremental Production Implementation to replace the legacy Shared Systems/CWF while maintaining continuity of Medicare Fee-for-Service operations. The contractor shall lead day-to-day delivery and coordinate with CMS, MACs, providers, and partner systems to achieve the outcomes below.

### MAC Onboarding

CMS intends to onboard MAC jurisdictions incrementally in production using a run-out strategy. For each MAC (or MAC region), CMS will designate a cutover Date of Service (DOS), and inbound claims routing will be based on DOS (not receipt date). Claims with a DOS prior to the cutover DOS will continue to be routed to, and processed by, the legacy environment with the legacy environment remaining the system of record for those pre-cutover services. Claims with a DOS on or after the cutover DOS will be routed to and adjudicated by ClaimsCore, with ClaimsCore serving as the system of record for those post-cutover services. Because claims may be submitted and paid after the service is furnished, CMS anticipates a run-out period during which the legacy environment remains available (operational and or accessible) to complete processing for pre-cutover DOS claims and to support provider inquiries, adjustments, appeals, audits, and legal or program integrity activities associated with the pre-cutover system of record. Contractors should not assume that ClaimsCore will be required to retroactively assume system-of-record responsibility for claims with DOS prior to the applicable cutover date, even if such claims are received after cutover.

Incremental MAC onboarding will create a temporary "split-history" operating state in which a beneficiary’s claims history and benefit accumulators are distributed across ClaimsCore and the Legacy Systems. During this hybrid period, beneficiaries may receive care in jurisdictions that have not yet cut over, jurisdictions processing on ClaimsCore, or both. Adjudication in either environment may require timely access to claim outcomes and beneficiary liability information

that resides in the other environment (e.g., prior payments and denials, duplicate or overlapping service checks, utilization and frequency limits, deductible and coinsurance accumulation). This split-history dependency introduces risk of incomplete information and inconsistent outcomes if cross-environment and cross-system claim outcomes are not available when needed to support claims processing and downstream activities (including provider and beneficiary inquiries, adjustments, appeals, audits, and program integrity or legal actions) that must rely on the applicable system of record. CMS anticipates that the legacy systems and ClaimsCore likely need to coordinate on claim outcomes and beneficiary state during the transition. Contractors should propose a strategy for ensuring timely coordination of adjudicated claims data between systems.

### Financial Disbursement and HIGLAS Integration

The contractor solution must integrate with CMS financial systems in production, including HIGLAS, to support payment authorization, accounting, reconciliation, and reporting, and must enable provider payment execution via electronic funds transfer through CMS- or Treasury-approved banking partners and/or coordination with MACs or CMS-designated services for paper check issuance. If this functionality is not provided out of the box, the contractor shall propose and implement compliant integrations or extensions to support uninterrupted Medicare Fee-for-Service payment operations, including required financial controls, auditability, and reconciliation.

### Tier 2-4 Integrations

CMS has defined 4 tiers of external systems required for parity. Tier 1 systems will have been completed during the proof of concept (though some interface mechanisms may need to change for the production phase), but during the production phase the contractor will complete the remaining 3 tiers including systems that less frequently impact the outcome of adjudication, MAC owned systems, and downstream data consumers. The contractor shall plan and deliver interfaces by tier, provide test packs, certification evidence, and error-budget reporting. The contractor shall also migrate, interface with, or virtualize historical and in-flight data required for operations, document mappings and lineage, execute reconciliation with defined tolerances and correct defects prior to cutover.

### Other Key Responsibilities

1. Maintain a single IMPS (which may be updated from the POC IMPS), define acceptance criteria for every workstream, update status, risks, and dependencies on the agreed cadence and make artifacts available to CMS.

2. Propose an IMPS-based milestone structure with objective evidence for acceptance (e.g., dual-run results, interface certifications, training completion, documentation delivered). Milestone payments are contingent on meeting the corresponding acceptance evidence.

3. Migrate, interface with, or virtualize historical and in-flight data required for operations; document mappings and lineage; execute reconciliation with defined tolerances and correct defects prior to cutover.

4. Maintain parity with legacy change requests during transition. For any policy, rules/edits, pricers, reference tables, or interface updates promoted in the legacy shared systems, implement the corresponding change in ClaimsCore within the QASP policy-agility cycle-time target, synchronize release dates, document and obtain CMS approval for any intentional deltas.

5. Training, communications, and change management Deliver role-based training for CMS and MAC users, publish job aids and cutover playbooks, and execute stakeholder communications to minimize operational impact.

6. Maintain continuous monitoring and ATO artifacts; meet vulnerability remediation timelines; implement business continuity and disaster recovery consistent with mission-critical objectives; perform scheduled failover/failback drills.

7. Provide runbooks, on-call and incident/problem/change management, deliver a post-go-live hypercare period for each cutover with active monitoring, variance remediation, and after-action reports.

8. Perform periodic export drills to a clean CMS tenant and rebuild as appropriate; provide vendor-neutral exports of data, rules, configurations, and integration assets to preserve portability.

9. Support CMS in retiring legacy components per the decommissioning plan as slices move to steady state.

10. For the duration of the contract, continue to configure the solution per CMS and MAC requirements and design, maintain, and evolve any required customizations, extensions, or integrations to support new or expanded CMS- or MAC-driven use cases, policy changes, operational needs, and external dependencies, while preserving upgradeability, performance, security, and alignment with CMS architectural and governance standards.

11. For the duration of the contract, fully manage the end-to-end cloud infrastructure for the solution, ensuring environments operate as expected scale elastically to meet demand, maintain high availability and resilience, and comply with CMS security, monitoring, and cost management requirements.

### Quality Control and Assurance

The Quality Assurance Surveillance Plan (QASP) identifies how, in part, CMS will evaluate the Contractor's performance. While the measures contemplated by CMS for potential inclusion in the QASP are described in Appendix B, the Contractor should propose performance measures which correspond to tasks in the Performance Work Statement (PWS) and will allow the team to monitor and respond to real-time conditions (e.g., transaction times, accuracy, response times, user acceptance, app errors) and proactively detect and prevent adverse conditions (e.g., code defects, release bottlenecks) impacting performance. CMS will consider for adoption the measures proposed.

The Contractor is responsible for reporting on those measures specified by CMS in the QASP. The frequency of reporting actual performance should enable appropriate intervention, such as technical changes, process improvements, or changes in staffing, to meet the performance standard. The proposed measures should be based on industry standards (e.g., IT Infrastructure Library (ITIL), Control Objectives for IT, etc.). The QASP and evaluation process may be adjusted over time based on lessons learned. In addition, the QASP reporting outcomes and associated performance discussions (including retrospectives) may be used by the Government as input for past performance reporting.

In addition to the above, the QASP should describe:

- How the team (i.e., Government and contractor personnel) will work together
- How the team will treat data used to measure performance
- How the team identifies ways to improve efficiency and reduce risk, and
- How disputes will be resolved.
- What performance remedies, fee at-risk provisions, service level credits, or cure processes are appropriate

## Timeline

This procurement will be conducted as a challenge-based acquisition with three phases. Feedback will be continuously provided throughout the phase. After each phase CMS will down-select vendors.

1. Request for Proposal (RFP) Acquisition using the evaluation criteria described in the solicitation.
2. Proof of Concept (Base Period, ending Jan 1 '27): CMS anticipates not more than four participants. Awardee(s) must deploy their solution, integrate with Tier 1 Systems, process a limited set of CMS data to validate baseline capabilities relative to the Evaluation Metrics, and demonstrate key functionality to CMS and MAC stakeholders before advancing to production implementation.
3. Production implementation (Option Periods as described in the Solicitation): One vendor only. The selected awardee will complete installation, integrate with all relevant external systems, and process CMS claims data according to its rollout plan.
4. Transition to a follow-on Contract (Final Option Period unless sooner as directed by CMS): validate data submissions are complete and accurate; prove readiness to export & transition to a follow-on platform or contract; implement transition plan as required below.

## Conclusion

ClaimsCore is intended to enable near real-time adjudication and claim status, improve transparency of beneficiary obligation information at the point of care, strengthen payment integrity, and reduce provider administrative burden. The program replaces legacy mainframe-based shared systems with a secure, scalable platform designed to reduce operational risk and

long-term sustainment costs, to support faster configuration-based policy updates, and enable future innovation.

## Appendix A: Security Requirements

*Information Security and/or Physical Access Security*

Baseline Security Requirements

a. Applicability. The requirements herein apply whether the entire contract or modification (hereafter "contract"), or portion thereof, includes either or both of the following:
    i. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.
    ii. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
b. Safeguarding Information and Information Systems. All government information and information systems must be protected in accordance with HHS/ CMS policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:
    i. Protect the:
        - Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information.
        - Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
        - Availability, which means ensuring timely and reliable access to and use of information.

    ii. Categorize all information owned and/or collected/managed on behalf of HHS/CMS and information systems that store, process, and/or transmit HHS information in accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. Based on information provided by the ISSO, CISO, CMS SOP, or other representative, the impact level for each Security Objective (Confidentiality, Integrity, and Availability) and the Overall Impact Level, which is the highest watermark of the three factors of the information or information system are the following:
        - Confidentiality: [ ] Low [ x ] Moderate [ ] High
        - Integrity: [ ] Low [ x ] Moderate [ ] High
        - Availability: [ ] Low [ x ] Moderate [ ] High

- Overall Impact Level: [ ] Low [ x ] Moderate [ ] High

iii. Based on the agreed-upon level of impact, implement the necessary safeguards to protect all information systems and information collected and/or managed on behalf of HHS/CMS regardless of location or purpose.

iv. Report any discovered or unanticipated threats or hazards by either the agency or contractor, or if existing safeguards have ceased to function immediately after discovery, within one (1) hour or less, to the government representative(s).

v. Adopt and implement all applicable policies, procedures, controls, and standards required by the HHS/CMS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain all applicable security and privacy policies by contacting the CO/COR or HHS/CMS security and/or privacy officials.

c. Privacy Act. Comply with the Privacy Act requirements (when applicable), and tailor FAR and HHSAR clauses as needed.

d. Privacy Compliance. Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable HHS/CMS privacy policies, and complete all the requirements below:

i. Per the Office of Management and Budget (OMB) Circular A-130, Personally Identifiable Information (PII), is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: Social Security number, date and place of birth, mother's maiden name, biometric records, etc.

ii. Based on information provided by the ISSO, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:

[ ] No PII [ x ] PII

iii. The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether or not a full Privacy Impact Assessment (PIA) needs to be completed.

iv. If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information within [CMS to insert contract-specific timeline] after completion of the PTA and in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

v. The Contractor must support the agency in reviewing the PIA at least every three years throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

e. Controlled Unclassified Information (CUI). Executive Order 13556 defines CUI as "information that laws, regulations, or Government-wide policies require to have safeguarding or

dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR, part 2002) when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "handling" refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be:

i. Marked appropriately;
ii. Disclosed to authorized personnel on a Need-To-Know basis;
iii. Protected in accordance with NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations if handled by internal Contractor system; and Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Information and/or data must be disposed of in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

f. Protection of Sensitive Information. For security purposes, information is or may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
g. Confidentiality and Nondisclosure of Information. Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS must be used only for the purpose of carrying out the provisions of this contract and must not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its employees and subcontractors must be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

   The confidentiality, integrity, and availability of such information must be protected in accordance with HHS and CMS policies. Unauthorized disclosure of information will be subject to the HHS/CMS sanction policies and/or governed by the following laws and regulations:

   i. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
   ii. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
   iii. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

h. Internet Protocol Version 6 (IPv6). All procurements using Internet Protocol must comply with OMB Memorandum M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6).

i. Information and Communications Technology (ICT). ICT products and services from prohibited entities/sources must not be used/acquired in compliance with Public Law 115-232, Section 889 Parts A and B, FAR 4.21, FAR 52.204.23, FAR 52.204.24, and FAR 52.204.25. The contractor (and/or any subcontractor) must notify the government if they identify prohibited ICT products and/or services are used during the contract performance.
j. Government Websites. All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, HTTPS is not required, but it is highly recommended. Consult the HHS Policy for Internet and Email Security for additional information.
k. Contract Documentation. The Contractor must use provided templates, policies, forms and other agency documents found at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library to comply with contract deliverables as appropriate.

1. Standard for Encryption. The Contractor (and/or any subcontractor) must:

i. Comply with the HHS Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.
ii. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
iii. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and CMS-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).
iv. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificate from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR [CMS-provided delivery date].
v. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys http://csrc.nist.gov/publications/. Encryption keys must be provided to the COR upon request and at the conclusion of the contract.

l. Contractor Non-Disclosure Agreement (NDA). Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract must complete the CMS non-disclosure agreement. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

2. Training Requirements
   a. Mandatory Training for All Contractor Staff. All Contractor (and/or any subcontractor) employees assigned to work on this contract must complete the applicable HHS/CMS Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees must complete CMS Information Security Awareness, Privacy, and Records Management training at least annually, during the life of this contract. All provided training must be compliant with HHS training policies.
   b. Role-based Training. All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training annually commensurate with their role and responsibilities in accordance with HHS policy and the HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum.
   c. Training Records. The Contractor (and/or any subcontractor) must maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records must be provided to the CO and/or COR within 30 days after contract award and annually thereafter or upon request.
3. Rules of Behavior.
   a. The Contractor (and/or any subcontractor) must ensure that all employees performing on the contract comply with the HHS Information Technology General Rules of Behavior, and HHS Rules of Behavior for Privileged Users.
   b. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least annually thereafter, which may be done as part of annual CMS Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.
4. Incident Response
   a. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/ CMS IRT teams within 24 hours, whether the response is positive or negative.

      FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. In accordance with OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (PII),

an incident is "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" and a privacy breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose." For additional information on the HHS breach response process, please see the HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)."

b. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must:
    i. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
    ii. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor must send CMS approved notifications to affected individuals in accordance with the CMS Breach Analysis Team (BAT) instruction.
    iii. Report all suspected and confirmed information security and privacy incidents and breaches to the CMS Incident Response Team (IRT) via the CMS Help Desk (410) 786-2580 or CMS IT Service Desk (cms_it_service_desk@cms.hhs.gov), COR, CO, CMS SOP (or his or her designee), and other stakeholders, including breaches involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than one (1) hour, and consistent with the applicable CMS and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:
        - Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
        - Not include any sensitive information in the subject or body of any reporting e-mail; and
        - Encrypt sensitive information in attachments to email, media, etc.
    iv. Comply with OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, and HHS/CMS privacy breach response policies when handling PII breaches.
    v. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or

applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.

5. Position Sensitivity Designations

   All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract:

   a. Homeland Security Presidential Directive (HSPD)-12

      The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; OMB M-05-24; OMB M-19-17; FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; HHS HSPD-12 policy; and Executive Order 13467, Part 1 §1.2.

   b. Roster

      The Contractor (and/or any subcontractor) must submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to the COR and/or CO within a timeframe to be determined by CMS of the effective date of this contract. Any revisions to the roster as a result of staffing changes must be submitted within a timeframe to be determined by CMS of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.

      If the employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level.

6. Contract Initiation and Expiration

   a. General Security Requirements. The Contractor (and/or any subcontractor) must comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor must follow the HHS EPLC framework and methodology or the CMS SDLC, as amended and in accordance with the HHS Contract Closeout Guide (2012).

   b. System Documentation. Contractors (and/or any subcontractors) must follow and adhere to HHS System Development Life Cycle requirements, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC and CMS SDLC that require artifact review and approval.

   c. Sanitization of Government Files and Information. As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) must provide all required documentation in accordance with the CMS SDLC, as Amended to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

d. Notification. The Contractor (and/or any subcontractor) must notify the CO and/or COR and system ISSO within as soon as possible or as determined by CMS before an employee stops working under this contract.
e. Contractor Responsibilities upon Physical Completion of the Contract. The contractor (and/or any subcontractors) must return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor must provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or CMS policies.
f. The Contractor (and/or any subcontractor) must perform and document the actions identified the COR when an employee terminates work under this contract within 30 calendar days of the employee's exit from the contract. All documentation must be available to the CO and/or COR upon request.

7. Records Management and Retention
   a. The Contractor (and/or any subcontractor) must maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS Policy for Records Management and CMS policies and must not dispose of any records unless authorized by HHS/CMS.
   b. In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS/CMS policies.

### *High Value Asset (HVA)*

If a system is identified as HVA, the contractor must comply with the HHS Policy for the High Value Asset (HVA) Program and the DHS HVA Control Overlay in addition to the above requirements.

### *Privacy Act Records*

### Privacy Act

It has been determined that this contract is subject to the Privacy Act of 1974, because this contract provides for the design, development, or operation of a system of records about individuals from which records are retrieved by name or other identifying particular.

The System of Records Notice that is applicable to this contract is:

- (09-70-0501) DMS - Multi-Carrier Claims System (MCS)
- (09-70-0503) Fiscal Intermediary Shared System (FISS)
- (09-70-0526) Common Working File (CWF)

- (09-70-0136) Durable Medical Equipment Claims System (DME)

The system of records design, development, or operation work the Contractor is to perform is:

The information collected, maintained or disseminated includes name, date of birth, Medicare Beneficiary Identifier (MBI), health insurance claim number, mailing address, phone numbers, medical record numbers, medical notes, bank account information and/or numbers, certificates, email addresses, military status and/or records, employment status and/or records, employer or school name, education records, medical notes, health insurer name/plan, health insurer group number, patient name, marital status, and employment status, financial account info, device identifiers, diagnosis and procedure codes, place of service codes, and provider name and address. User's ID and passwords also reside and are managed by DME. The DME user's IDs and passwords are synchronized by the CMS Enterprise User Administrator system (EUA) to CMS user IDs.

N/A for Development DME

The disposition to be made of the Privacy Act records upon completion of contract performance is:

All data in DME system will be disposed of in accordance with the National Archives and Records Administration (NARA) Disposition Authority DAA-0440-2015-0006 which has 7-year minimum retention. Data in DME system can be divided into three categories:

• External Input Data

• DME database data

• External Output Data

1. Security Requirements for GOCO and COCO Resources
    a. Federal Policies. The Contractor (and/or any subcontractor) must comply with applicable federal laws and HHS policies that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)*, *CMS Information Systems Security and Privacy Policy (IS2P2), Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, *Security and Privacy Controls for Information Systems and* Organizations; Office of Management and Budget (OMB) Circular A-130*, Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
    b. Assessment and Authorization (A&A). A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to

protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) must work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) to be determined by CMS. The Contractor must conduct the A&A requirements in accordance with *HHS IS2P/ CMS IS2P2*, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach* (latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision).

CMS acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

i. A&A Package Deliverables - The Contractor (and/or any subcontractor) must provide an A&A package within as determined by CMS to the CO and/or COR. The following A&A deliverables are required to complete the A&A package :

   - System Security Plan (SSP) – due prior to the submission of the A&A package in order to request an ATO, based on the CFACTS format template. The SSP must comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and CMS policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor must review and update the SSP at least ***annually*** thereafter and if requested, provide a copy of the updated SSP.
   - Security Assessment Plan/Report (SAP/SAR) - due prior to the ATO. The security assessment must be conducted by a third party assessor for High and Moderate systems, or by an independent assessor for Low systems and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and CMS policies. The assessor will document the assessment results in the SAR.

     Thereafter, the Contractor, in coordination with CMS must assist in

the assessment of the security controls initially and update the SAR at least ***annually***. A copy of the updated SAR should be provided if requested.

- Independent Assessment – due as required by CMS. The Contractor (and/or subcontractor) must have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party must review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor must address all *"high"* deficiencies before submitting the package to the Government for accreditation and/or acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).
- POA&M – due within 30 days after the independent third-party assessment final report approval and must be created in CFACTS. All critical-risk weaknesses must be mitigated within ***15 days,*** high-risk weaknesses must be mitigated within ***30 days***, medium weaknesses must be mitigated within ***90 days,*** and low weaknesses must be mitigated 365 days, from the date the weaknesses are formally identified and documented. CMS will determine the risk rating of vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, must be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones and CMS policies. Depending on the severity of the risks, CMS may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document must be updated at least quarterly in CFACTS.
- Contingency Plan and Contingency Plan Test – due prior to the ATO and updated annually thereafter. The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and CMS policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, must test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any

action items that need to be addressed. Thereafter, the Contractor must update and test the Contingency Plan at least ***annually***.

- E-Authentication Questionnaire - The contractor (and/or any subcontractor) must collaborate with government personnel to ensure that the E-Authentication requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 B.

  Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS *Guidance for Selection of e-Authentication Assurance Levels* and any other applicable HHS/CMS policies.

ii. Information Security Continuous Monitoring. Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, must meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, HHS ISCM Strategy, HHS IS2P and CMS IS2P2.

iii. Annual Assessment/Penetration (Pen) Test - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the agency or independent third-party.) In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date to be determined by CMS.

iv. Asset Management - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS/CMS-owned information/data. It is anticipated that this inventory information will be required to be produced at least every 72 hours. IT asset inventory information must include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor must maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the *HHS Policy for Information Technology Asset Management (ITAM)* and any other applicable HHS policy.

v. Configuration Management - Use available SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to: computers, servers, routers, databases, operating systems, application, etc., that store and process government information. Provide scan reports to HHS/CMS upon request. The contractor must maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

vi. Vulnerability Management - Contractors must actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor must maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least every 72 hours.

vii. Patching and Vulnerability Remediation - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and CMS specified timeframes:
   - Critical vulnerabilities require patching to be released and remediated within 15 days
   - High vulnerabilities require patching to be released and remediated within 30 days

viii. Secure Coding - Follow the *HHS Policy for Software Development Secure Coding Practices* and secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.

ix. Boundary Protection - The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).

c. Government Access for Security Assessment. In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) must afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS/CMS, including but are not limited to:

   i. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's

direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.

ii. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

- Segregate Government protected information and metadata on the handling of Government protected information from other non-government information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.
- Cooperate with inspections, audits, investigations, and reviews.

d. End of Life Compliance. The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO if it impacts enterprise-wide systems and services, or by the CMS CISO if it impacts only the

CMS). The contractor must retire and/or upgrade all software/systems that have reached end-of-life in accordance with *HHS End of Life Operating Systems, Software and Application Policy*.

e. Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor. The Contractor (and/or any subcontractor) must ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS/CMS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:
    i. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with CMS, HHS encryption standard and current FIPS 140 validation certificate from the NIST CMVP.
    ii. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), in accordance with Acceptable Risk Safeguards (ARS) control CM-6, Configuration Settings, other CMS settings requirements, and HHS Minimum Security Configuration Standards;
    iii. Maintain the latest operating system patch release and anti-virus software definitions*;*
    iv. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
    v. Automate configuration settings and configuration management in accordance with HHS/CMS security policies, including but not limited to:
        - Configuring its systems to allow for periodic HHS/CMS vulnerability and security configuration assessment scanning; and
        - Using Security Content Automation Protocol (SCAP)-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

f. Rights to Data. All contracts that require data to be produced, furnished, acquired, or used in meeting contract performance requirements, must contain terms that delineate the respective rights and obligations of the Government and the contractor regarding the use, reproduction, and disclosure of that data. Data rights clauses do not specify the type, quantity or quality of data that is to be delivered, but only the respective rights of the Government and the contractor regarding the use, disclosure, or reproduction of the data. Accordingly, the contract must specify the data to be delivered.

g. Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements. The Contractor (and/or any subcontractor) must secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232 § 889. At a minimum, they must implement the following:

i. Develop rules for suppliers' development methods, techniques, or practices;
ii. Use of secondary market components;
iii. Prohibit counterfeit products;
iv. Dispose and/or retain elements such as components, data, or intellectual property securely;
v. Ensure adequate supply of components;
vi. Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;
vii. Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;
viii. Establish Service Level Agreements (SLAs), patching vehicles and disclosure requirements in the case of a security incident or new vulnerability being discovered; and
ix. Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and
x. Prohibit the use of covered telecommunications and video surveillance equipment or services.

### *Contracts Involving Cloud Services*

1. HHS FedRAMP Privacy and Security Requirements

   The Contractor (and/or any subcontractor) must be responsible for the following privacy and security requirements:

   a. FedRAMP Compliant ATO. Comply with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO by a timeline determined by CMS.
      i. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The HHS Information Security and Privacy Policy (IS2P), HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance, and the CMS Information System Security and Privacy Policy (IS2P2) further define the baseline policies as well as roles and responsibilities. The Contractor must also implement a set of additional controls identified by the agency when applicable.

ii. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

b. Data Jurisdiction. The contractor must store all information within the security authorization boundary, data at rest or data backup, within the Continental United States (CONUS) if so required. Refer to G. Contractor Work Performed Outside of the United States and its Territories (April 2016) in the Solicitation/Contract.

c. Service Level Agreements. Add when applicable The Contractor must understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with CMS to develop and maintain an SLA.

d. Interconnection Agreements/Memorandum of Agreements. Add when applicable The Contractor must establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/CMS policies.

2. Protection of Information in a Cloud Environment

a. If contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they must protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/CMS policies https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html.

b. HHS/CMS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS/CMS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS/CMS and hosted on contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS/CMS within one (1) business day from request date or within the timeframe specified otherwise. In addition, the data must be provided at no additional cost to HHS/CMS.

c. The Contractor (and/or any subcontractor) must ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS/CMS policies.

d. The contractor must support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:

i. Maintenance of links between records and metadata, and

ii. Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

e. The disposition of all HHS/CMS data must be at the written direction of HHS/CMS. This may include documents returned to HHS/CMS control; destroyed; or held as specified until otherwise directed. Items returned to the Government must be hand carried or sent by certified mail to the COR.
    i. If the system involves the design, development, or operation of a system of records on individuals, the Contractor must comply with the Privacy Act requirements.

3. Assessment and Authorization (A&A) Process
    a. The Contractor (and/or any subcontractor) must comply with HHS/CMS and FedRAMP requirements as mandated by federal laws, regulations, and HHS/CMS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS/CMS security policies. The contractor must obtain authorization prior to deployment or service implementation.
        i. In addition to the FedRAMP compliant ATO, the contractor must complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation within CFACTS in a timeline to be determined by CMS. The agency ATO must be approved by the CMS authorizing official (AO) prior to implementation of system and/or service being acquired.
        ii. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO but should not use self-assessment. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
        iii. For all acquired cloud services, the A&A package must contain the following documentation:
            - Security Assessment Plan (SAP)/Security Assessment Report (SAR)
            - System Security Plan (SSP)
            - Plan of Action and Milestones
            - Contingency Plan and Contingency Plan Test
            - E-Authentication Questionnaire].

        Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/CMS policies using CMS templates and defined timelines.

    b. HHS/CMS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS/CMS exercises this right, the Contractor (and/or any subcontractor) must allow HHS/CMS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS/CMS requirements. Review activities

include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

c. The Contractor must identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the contractor must document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS/CMS may require remediation at the contractor's expense, before HHS/CMS issues an ATO.
d. The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings must be remediated, in accordance with timelines specified in the HHS POA&M Standard, from discovery: (1) critical vulnerabilities no later than fifteen (15) days and (2) high within thirty (30) days (3) medium within ninety (90) days and (4) low vulnerabilities no later than three hundred and sixty (360). In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the timelines assigned to the POA&M within CFACTS. HHS/CMS will determine the risk rating of vulnerabilities using FedRAMP baselines.
e. Revocation of a Cloud Service. HHS/CMS have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS/CMS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or CMS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

4. Reporting and Continuous Monitoring
    a. Following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities. Meetings shall be held at least monthly, or as needed.

b. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis via the CCIC requirements which can be provided by contacting EVM-CMP@cms.hhs.gov. Deliverables are identified as:
    i. Operating system, database, Web application, and network vulnerability scan results;
    ii. Updated POA&Ms;
    iii. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the CMS System Owner or AO; and
    iv. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/CMS security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.

5. Configuration Baselines.
    a. The contractor must certify that applications are fully functional and operate correctly as intended on systems using HHS Minimum Security Configurations Standards Guidance. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS/CMS configuration baseline.
    b. The contractor must use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS/CMS and NIST defined configurations and do not alter these settings.
6. Incident Reporting

    a. The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS/CMS], OMB, and US-CERT requirements and obtain approval from CMS. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.
    b. The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS/CMS access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection must include, but is not limited to:

        i. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/CMS personnel, or agents acting on behalf of HHS/CMS, using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are

compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.

ii. In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes at a minimum the following:
    - Company and point of contact name;
    - Contract information;
    - Impact classifications/threat vector;
    - Type of information compromised;
    - A summary of lessons learned; and
    - Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.

7. Media Transport
    a. The Contractor and its employees must be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).
    b. All information, devices and media must be encrypted with HHS/CMS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

8. Boundary Protection: Trusted Internet Connections (TIC)
    a. The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes that are in compliance with the requirements of the Office of Management and Budget (OMB) Memorandum (M) 19-26: Update to the TIC Initiative, TIC 3.0.
    b. The contractor must route all external connections through a TIC.
    c. Non-Repudiation. The contractor must provide a system that implements encryption with current FIPS 140 validation certificate from the NIST CMVP that provides for origin authentication, data integrity, and signer non-repudiation.

## Appendix B: QASP

| Deliverable / Area | Performance Standard(s) | Acceptable Quality Level (AQL) | Method of Assessment | Reporting Frequency |
|---|---|---|---|---|
| Integrated Master Plan & Schedule (IMPS) | On schedule based on CMS IMPS/WBS; each WBS element has acceptance criteria; update weekly; no stage moves without evidence. | 100% of WBS items have acceptance criteria; ≥95% weekly updates on time; on schedule | IMPS/WBS audit; spot checks of acceptance evidence. | Weekly during Base Period and MAC onboarding and validation period |
| Parallel-run alignment | Claim-level outcome alignment for in-scope slice | ≥ 95% of claims aligned per validation criteria; remaining differences fully explainable | Varience analysis regression packs; difference taxonomy with root-cause | Weekly during Base Period and MAC onboarding and validation period |
| System Uptime | Vendor system fully online, able to process claims; provide expected functionality | 99.9% uptime monthly (max. 43 min 12 sec downtime/mo.). Excludes scheduled maintenance windows. | Cloud/APM monitoring, synthetic probes | Real-time dashboard; Monthly report |
| Claims Processing Time | Low Latency | p95 ≤ 1s, p99 ≤ 2s adjudication for clean claims (measured within vendor boundary); | End to End measurement | Real-time dashboard showing time in vendor boundary, and round-trip time for external API calls; Monthly report |
| Claims Processing Load | High Throughput | System sustains 400,000 transactions per hour | Detect lost claims or breaches of latency at peak load times | Real-time dashboard; Monthly report |
| Customer Satisfaction Score (CSAT) | Customer satisfaction with specific interactions (e.g., support, onboarding, feature usage). | >75% average across questions | Stakeholder Survey, questions scored 1-5; random sample of stakeholders | Monthly report |

| | | | | |
|---|---|---|---|---|
| UI Responsiveness (Perceived Performance) | Key user interface actions and screen loads respond quickly under typical load conditions to ensure efficient user workflow. | p90 ≤ 1s for key user actions (e.g., dashboard load, claim search results, saving a form). | Browser performance monitoring (BPM), synthetic monitoring of key user journeys. | Real-time dashboard; Monthly report |
| Recovery Time Objective (RTO) | Time taken to restore the claims system to full operational status after a declared disaster event. | RTO ≤4 hour from declaration of disaster for mission-critical functions. | Documented disaster recovery (DR) test results and incident response logs. | Tested semi-annually; results reported within 24 hours of test/incident. |
| Recovery Point Objective (RPO) | Maximum allowable amount of data loss (measured in time) after a disaster event. | RPO ≤ 15 minutes of data loss during any disaster recovery scenario. | Data backup logs, replication logs, and validation during quarterly DR tests. | Tested semi-annually; results reported within 24 hours of test/incident. |
| Change failure rate | Production releases or change requests causing degraded service (rollback/hotfix). | ≤ 5% of changes | Release records; incident/problem mgmt. | Monthly |
| Time to restore service (MTTR) | From outage ticket open to service restored. | 95% restored within contracted times for well-defined priority levels | ITSM reports; incident postmortems. | Monthly. |
| Security: vulnerabilities & ATO | FedRAMP/CMS ARS compliance; vulnerability remediation. | No open Critical/High at go-live; remediation timelines: Critical ≤ 15 days, High ≤ 30 days; POA&M items on-time; SCA/ACT pass. | Scan reports; POA&M; SSP/SAP/SAR reviews. | Monthly scans; scans on code changes; POA&M monthly. |
| Integration Turnaround Time | Time from formal requirement sign-off to successful deployment of a new external system integration into production. Measurement pauses during periods of documented delay caused solely by the external integration partner (e.g., partner failed to provide access, testing | Average ≤ 60 business days for standard integrations (measured only for time within provider's control). | Project management system logs, documented communication records (emails, meeting notes) with partners, deployment records, and project | Monthly report on integration projects, including variance explanations for delays caused by external partners. |

| | | | | |
|---|---|---|---|---|
| | delays on their end, data format issues from their system). | | completion sign-off dates. | |
| Rule transparency & traceability | Complete documentation and change history for edits/rules. | 100% of production rules have human-readable spec + machine-readable config, test cases, and change log. | Repo/Confluence review; spot checks in demos. | Monthly report on new changes |
| Testing health | Automated test coverage & pass rate for custom code/integration. | ≥ 90% line/branch coverage; ≥ 95% pass rate; flakiness < 2%. | CI pipeline reports; test dashboards. | Per PR and per release. |
| User research & usability | Continuous research & periodic usability testing for user-facing flows. | Artifacts available per research plan; ≥ 85% CSAT on evaluated workflows. | Manual artifact review; survey results. | Per applicable sprint/release. |
| Training & adoption | Role-based training for CMS/MAC users. | ≥ 90% training completion in targeted audience; ≥ 85% learner satisfaction. | LMS export; Training survey results. | Per rollout wave. |
| Help desk responsiveness | Ticket response and resolution SLAs. | 95%: respond ≤ 1 hr.; resolve: Tier1 ≤ 6 hrs., Tier2 ≤ 2 biz days, Tier3 ≤ 5 biz days. | ITSM reports; QBR review. | Monthly. |
| Cloud cost efficiency | Instance currency, right-sizing, utilization, discounts. | Optimize cloud footprint and usage to CMS published cloud OKRs | Automated cloud inventory & cost reports. | Monthly. |
| Portability drills | Annual export to clean CMS tenant (data + config + rules + integration assets). Rebuild where appropriate. | 100% drill completion; export completeness ≥ 99.9%; rebuild executable in ≤ 48 hrs.; drill AAR with gap closure plan. | Drill runbooks; export checksums; rebuild logs; AAR. | Annual. |

| | | | | |
|---|---|---|---|---|
| Reporting | Program visibility: status, metrics, risks, financial status (burn rates). | 100% on-time Monthly Status Report and live dashboards accessible to COR/PO; IMS updated to current baseline. | MSR + dashboard review; IMS diff. | Monthly (status); continuous (dashboards). |
| The Definition of Done (DoD) | The deliverables for each sprint, integration, or work product meets the Definition of Done as defined collaboratively between Contractor and CMS | 100% | Combination of manual review and automated testing | Monthly |
| Option-year gate readiness package | Provide a single scorecard showing results vs. gate thresholds (accuracy, alignment, uptime/latency, Tier-1 certs, DR drill pass, training completion/CSATCSAT) to support exercise/non-exercise decisions. | All thresholds met for gate approval; if any fail, deliver a Performance Improvement Plan (PIP) with package. | Gate packet with objective evidence; COR/CMS Leadership review; contract file. | End of Base Period and Option Years |

## Appendix C: Features and Functionality

CMS will assess the breadth, depth, and configurability of the platform's native feature set relevant to Medicare Fee-for-Service claims processing and operations. At a minimum, a production ready system SHOULD implement each of the features listed below. CMS will assess how robust and production-ready the capabilities are (e.g., claims intake and routing, rules/configuration model, explainability, operations tooling, reporting/analytics, admin and governance features) and the extent to which needs can be met through configuration rather than customization.

| Function | Description |
|---|---|
| 276/277 Claims Status | HIPAA Transactions and Code Sets compliance is required for all claim types. |
| Coordination of benefits | Fully integrate with the Coordination of Benefits Contractor (COBC) and be able to accurately send COB outbound claims for secondary payers. Includes importing information from beneficiary records currently in the Common Working File (CWF) as to which benes have a secondary payer. |
| Medicare Secondary Payer Integration | Accurately access MSP information and calculations |

| | |
|---|---|
| Full Claims Data Visible on User Screens - All data elements from 837P/1500 and 837I/UB-04. | Users can see all claims data, both submitted and created by the system, on screens so that adjudicators can see and understand what happened on a claim. |
| Implementation of Medicare Administrative Contractor (MAC)-Controlled Edits | MACs need to be able to have the flexibility to create and control edits under their purview. This includes porting over current editing from the MCS/DME SPITABs, FISS ECPS events, and other such systems. |
| Full implementation of cross-system edits | Able to ensure that the same claim cannot be paid from the future system or other systems during transition. |
| Integration with HIPAA Eligibility Transaction System (HETS) | This is CMS' current implementation of 270/271 eligibility transaction, a HIPAA Standard transaction. HIPAA Transactions and Code Sets compliance is required for all claim types. |
| Able to identify scenarios when processing a claim requires adjustments to previously paid claims | Able to read history of all processed claims when a new claim is added to history and to ensure proper adjusting of previously processed claims when necessary. (Analog to current CWF informational unsolicited response (IUR) requirements.) |
| Comprehensive Adjustment Functionality | MACs need to be able to adjust claims, either fully or partially, and initiate those adjustments either manually or via a mass adjustment process. Full cancellation claims must also be supported. |
| Claims History Storage & Search Capabilities | All claims need to be stored and searchable by the MACs and the CSRs. |
| Beneficiary-based Edits Functionality | The system needs to edit against all beneficiary entitlement, enrollment, benefit election and utilization (analog to current CWF beneficiary master record and auxiliary files). The system needs to update those files as appropriate so that future claim types pay correctly. |
| Application of beneficiary liability amounts | The system must accurately track and apply all beneficiary deductible and coinsurances amounts. It also assigns provider or beneficiary liability accurately in Advanced Beneficiary Notice (ABN) situations based on the submitted modifiers on occurrence codes. |
| Validation of Providers Using the Provider Enrollment Chain and Ownership System (PECOS) | PECOS is the system of record for provider enrollments, updates based on new information submissions, provider relationships and payment suspensions. National Provider Identifiers must be validated against PECOS information differentially when billing vs. rendering provider. |
| National Correct Coding Initiative (NCCI) Edit Functionality | The system needs to be able to accept/use the quarterly NCCI edit files, and properly access/apply edits to all dates of service. |
| Medically Unlikely Edits (MUEs) | The system needs to be able to accept/use the quarterly MUE edit files, and properly access/apply edits to all dates of service. |
| Fraud Prevention System (FPS) Integration | The system needs to be able to fully integrate with FPS editing |
| Merit-Based Incentive Payment System (MIPS)/Other Quality Payment Systems | The system needs to be able to apply payment adjustments for the MIPS/other systems, including proper reporting to the provider on |

| | |
|---|---|
| | the remit, and share data with those systems to ensure providers are properly reimbursed. |
| CMS1490S/Beneficiary Claims | The system needs to be able to accept/process beneficiary-submitted professional claims. |
| Full integration with Healthcare Integrated General Ledger Accounting System (HIGLAS) | The system should be able to directly interface with HIGLAS, which is required for compliance with statutory reporting requirements and interactions with the Treasury. |
| Workload Reporting (CROWD & CMS ARTS) | The system should supply similar data in a timely fashion to allow MACs to continue contractually required reporting of data to CMS. |
| Roles-Based Adjudication Permissions | The system must allow for the assignment of roles-based permissions for claims examiners, CSRs, managers, financial personnel, and others in a similar fashion to that which exists in the Legacy Systems today. |
| Full Integration with Medicare Appeals System (MAS)/Appeals Functionality | The system must allow for full appeals tracking and functionality, including support of redeterminations, reopenings and higher-level appeals. |
| Full Claims History Sharing Across MACs | In order to assure correct payment and prevent fraud, the system must integrate payment of all claim types by all MACs to ensure that claims are paid in once and only once. |
| Full Integration of Medicare Physician Fee Schedule (MPFS) and Other Fee Schedules | The system must be able to ingest and apply proper payments and payment indicators from the MPFS and other fee schedules. This includes all indicators currently present on the MPFS and other fee schedules; includes integration with PCS. |
| Interface with patient assessments in the internet Quality Improvement Evaluation System (iQIES) | Data exchange between the claims system and iQIES provides data elements required to execute the HH Grouper program and validates payment groups for inpatient rehabilitation facility claims |
| Full Integration of Institutional Claim Groupers and Code Editors | Institutional inpatient claims must process through the Medicare Code Editor (MCE), institutional outpatient claims must process through the Integrated Outpatient Code Editor (IOCE), and all claims must use the Grouper program appropriate to the Type of Bill. |
| Full Integration of Institutional Pricing Software | Institutional claims must integrate with all Original Medicare Pricer programs as appropriate for the Type of Bill |
| Implementation of All Rules for Prospective Payment System (PPS) Processing | Many, complex rules enforce PPS processing rules and ensure claims are not paid separately under bundling or consolidated billing rules. |
| Application of Value-Based Purchasing (VBP) and Quality Reporting Program (QRP) Payment Adjustments | Institutional provider files must support adjustment factors and payment indicators to supply Pricers with sufficient information to calculate VBP and QRP payments correctly. |
| Application of Coverage Policies for Durable Medical Equipment (DME) | The system must enforce purchase vs. rental rules, capped rental periods, maintenance payments, competitive bidding and various other DME-specific policies. |

| | |
|---|---|
| Assurance of Beneficiary and Provider Alignment with Innovation Center Models | The system must support functionality comparable to existing model alignment files and update claims with model information as needed. |
| Comply with all A-123 Rules/Control Objectives | The Contractor must have internal controls which comply with all OMB Circular A-123 requirements and permit assessment. These controls must ensure effective and efficient operations, legal compliance, and reliable financial reporting. |
| Full Implementation of all Claims Processing Rules Contained in the Medicare Internet-Only Manuals (IOMs) and all published Change Requests | The system must be able to replicate all business rules currently contained in MCS, FISS, DMEDME and CWF and to add new business rules as required by CMS instructions. In the event rules conflict with published policy, regulation, or guidance contractors should work with CMS and MACs to establish the preferred implementation. |
| Full Implementation of Additional Documentation Requests (ADRs) | The system must be able to generate request letters for medical records and facilitate the use of received records to perform medical review. |
| Ability to perform full regression testing | Testing processes must be in place to ensure changes to do have unintended adverse impact on processes already in place |
| National Coverage Determination (NCD) Implementation Ability | The system must be able to implement new, complex NCDs efficiently. |
| Local Coverage Determination (LCD) Implementation Ability | The system must enable MACs to implement new, complex LCDs efficiently. |
| Use of Modifiers to Modify Payments | The system must adjust fee schedule payments when modifiers indicate special payment rules apply (examples: co-surgeon, multiple procedures, etc.), per CMS policy. |
| Claims Hold Capability | The system must easily enable MACs to hold claims, singly or in batches, when manual adjudication is required or when directed to hold claims by CMS. |
| Downstream Data Systems | All claims must be sent to the Recovery Audit Contractor Data Warehouse (RACDW), Chronic Conditions Warehouse (CCW), Integrated Data Repository (IDR), either directly or transitively. This data needs to be shared timely with CMS' data systems for use by the Office of the Actuary, researchers, rate setters, quality programs and other users. |
| Support for Cost Reporting Processes for Institutional Providers | The system must pass claims data to the Provider Statistical and Reimbursement (PS&R) system to enable providers to complete cost reports. The system must enable payment holds for failure to submit cost reports and payments/withholding that reflect the settlement of cost reports. |
| Support for Periodic Interim Payments (PIP) for Institutional Providers | The system must generate period interim payments to certain providers, process corresponding claims without issuing payment and reconcile calculated claim amounts with PIP payments periodically. |
| Well-defined, repeatable change management process and documentation of | Full integration into the existing software development lifecycle (SDLC) structure |

| | |
|---|---|
| business and technical requirements | |
| Flexible search capabilities | The system must have ability to search for claims and documentation in various ways, including by beneficiary identifier, provider identifier or claim internal control number (ICN) |
| Health Professional Shortage Area (HPSA) Bonus Reporting | The system must calculate HPSA bonuses accurately based on provider locality, reflect payments accurately on remittances and produce reports for CMS monitoring of the number of HPSA providers. |
| Full Support of Electronic Provider Payments | The system must support Electronic Funds Transfer to provider accounts and compliant 835 remittance advice generation with appropriate group codes, claim adjustment reason codes and remittance advice remark codes explaining all payments and denials. |
| Generation of Beneficiary Notices | The system must generate and support mailing of the required Medicare Summary Notice (MSN) format |
| Full Audit Trail Capabilities | The system must record all processing steps and adjudication events so that detailed history is available for research of individual claims. |
| Customer Service Functionality | MAC business functions, including contact centers, must have ability to get information about claims. This functionality also feeds self-service portals and IVRs. |
| Role-based access control and PHI protection. | The system must support all security measures in the NIST SP 800-53 framework, including role-based access control so that users cannot exceed their scope of duties or operate the system in areas outside their functional responsibilities. This must include defining PHI access by specific roles. |
| FISMA/NIST 800-53 requirements validation. | The system must comply with all mandatory cybersecurity standards for federal agencies and allow for assessment against the security controls outlined in NIST Special Publication 800-53, which are required by the Federal Information Security Modernization Act (FISMA) |

## Appendix D: Tier 1 Systems List

| System/Center | Description |
|---|---|
| EDI Gateway | Primary entry point for electronic Medicare claims; validates HIPAA compliance and routes claims to processing systems |
| EDB/CME | Enrollment Database / Common Medicare Environment. Centralized repository for all Medicare provider/supplier enrollment data; single source of truth for provider information |
| PECOS | Provider Enrollment, Chain, and Ownership System. Web-based enrollment application system; manages provider enrollment, revalidation, and organizational relationships |
| Pricers, Coding & Fee Schedules | Integrated payment calculation systems using coding standards and fee schedules to determine accurate Medicare reimbursement |

| | |
|---|---|
| FPS | Fraud Prevention System. Predictive analytics platform using machine learning to identify and prevent fraudulent claims before payment |
| CM/CMMI | Center for Medicare / Center for Medicare and Medicaid Innovation. Innovation center testing new payment and delivery models to improve quality and reduce costs; scales successful innovations |
| PSF | Provider Screening Framework. Risk-based provider screening framework using verification, background checks, and site visits to prevent fraudulent enrollment |
| MSP Data | Medicare Secondary Payer Data. Tracks beneficiary other insurance coverage to ensure proper coordination of benefits and Medicare secondary payer compliance |
| HPMS | (Under Evaluation) Health Plan Management System. Comprehensive management platform for Medicare Advantage and Part D plans; handles bids, contracts, and compliance |
| IDR | (Under Evaluation) Integrated Data Repository. Enterprise data warehouse consolidating Medicare data from all sources; supports analytics, reporting, and research |

## Appendix E: General CMS & Related Technical Standards

The Contractor should perform all work associated with this effort in a manner consistent with the requirements, methods and/or goals described in the following references:

- Digital Services Playbook
- Developer tools from Centers for Medicare & Medicaid Services: collection of APIs, datasets, frameworks, and style guides
- The Agile Manifesto
- The TechFAR Hub
- 18F API Standards
- White House API Standards
- Building the Twelve-Factor App
- Scaled Agile Framework (SAFe) Agile Framework
- Federal Cloud Computing Strategy "Cloud Smart"
- CMS Target Life Cycle (TLC) guidelines
- Section 508 at CMS
- CMS Information Security and Privacy
- Overarching CMS IT Guidelines
- Design Guidance at Digital.gov
- CMS Web Design System(s)
- CMS Data Administration framework: CMS guidance to support consistent creation, utilization, and maintenance of CMS data resources.
- Cybergeek (for IT Security Policy)
- CMS Share IT Act Resources
- CMS' open source policy and helpful resources from the Digital Service at CMS (DSAC)
- Artificial Intelligence at CMS
- CMS Technical Reference Architecture

- Data.CMS.gov: This site gives you direct access to public data released by the Centers for Medicare & Medicaid Services (CMS), including beneficiary enrollment.

## Appendix F: MAC Statements of Work

A list of the functions of Medicare Administrative Contractors by jurisdiction. The Statement of Work (SOW) can be found in the attachments section at the bottom of each webpage. Occasionally the SOW is posted independent of the procurement documents, however, most commonly they are included in the RFP package attachments (zip file).

ClaimsCore offerors may find other documents in the package useful for a better understanding of workloads (J.22 Basis of Estimate) and technical assumptions relevant to MACs (J.23 Government Provided Proposal Assumptions).

JH 2024: https://sam.gov/workspace/contract/opp/0c758f8132e64787a0cb815142ac50d9/view

JF 2024 https://sam.gov/workspace/contract/opp/d8c8d79b40544fd885cb4ed6499f1550/view

JL 2020 https://sam.gov/opp/909db66e899e44acb137179138ebd50f/view

JN 2021 https://sam.gov/opp/87317852c030471f8f1cef264ee5ef5c/view

JE 2019
https://sam.gov/opp/ed54103c49052df3e18e622fa813d4eb/view?keywords=75FCMC19R0023&sort=-relevance&index=&is_active=false&page=1

JJ 2023 https://sam.gov/opp/a6df23d99aed4b0bb837a19eb4f9e5bf/view

JM 2022 https://sam.gov/opp/109fa666b2854e979e18e76ab17c8644/view

J15 2022 https://sam.gov/opp/6fa925fae9e4459294a58dad8ffefef0/view

J5 2018 https://sam.gov/opp/3d8ff4a6b5635df755d4ba7a005b4c3b/view

J6 2019
https://sam.gov/opp/ba9b2e291b8dd81e1c195aa066a882c5/view?keywords=75FCMC19R0002&sort=-relevance&index=opp&is_active=false&page=1

JK 2020 https://sam.gov/opp/b3ca6f1a27f34950b9d28374d03a8ad2/view

J8 2017 https://sam.gov/opp/f7d62fc4ab22c6668cfbb450a2848c06/view?keywords=%20RFP-500-2017-0016&sort=-relevance&index=&is_active=false&page=1

## Appendix G: Specialty Workloads

More information on these workloads can be found in the MAC Statements of Work linked in Appendix F.

C.7 Jurisdiction-Specific Requirements

C.7.1 Centralized Billing for Mass Immunizers (JH)

C.7.2 Indian Health Services (JH)

C.7.5 Veterans Affairs Medicare Equivalent Remittance Advice Project (JH)

C.7.11 Medicare Part B Drug Code Crosswalk File (JM)

C.7.14 Limited Purpose Insurance Company (JJ)

C.7.15 Independent Organ Procurement Organizations (JJ)

C.7.16 Religious Non-Medical Health Care Institutions (JJ)

C.7.17 Histocompatibility Labs (JJ)

C.7.18 Spanish Translation of HCPCS Code Descriptors (JN)

C.7.19 High Risk Fraud, Waste, or Abuse Areas (JE, JH, JK, JN and J8)

C.7.24 Medicare Pilot Project for Asbestos Related Disease (MPPARD) (aka Libby) (JF)

C.7.29 Medicare Essential Hospital Payment Program (MEHPP) (JF)

C.7.34 Records Storage & Retrieval Cost for non-J5 Legacy A Records (J5)

C.7.37 Mayo Clinic Project (J6)

C.7.38 Molecular Diagnostic Testing (MDT) Pricing Project (MolDx) (JM)

C.7.43 PECOS SME (J15)

C.7.44 Medicare Ground Ambulance Initial Data Collection (J (JJ))