

I.D.	Category	Subcategory	Requirement	Requirement Description
1	Cost Allocation Methodology	Assignment Methods (Direct Trace, Relational, General Allocation)	The system shall support many to one [e.g., intermediate products (IP) to a department] relationships as business needs require.	The system shall allow as many IPs as required to be mapped to a single department as well as associating unique combinations of feeder keys, feeder locations, and feeder systems (called an interface) with a single IP number.
2	Cost Allocation Methodology	Assignment Methods (Direct Trace, Relational, General Allocation)	The system shall allow for the creation of multiple overhead cost pools with different cost drivers [e.g., total cost, full time equivalents (FTE), percentages, etc.] and cost objectives to allocate indirect costs based on business rules.	There are varying methods of allocating overheads, however the allocation of non-local overhead costs is standardized across the VA network--despite some differences between the various national overheads. National, regional, Veteran Integrated Service Network (VISN), and other overhead costs are allocated to all, or specific VA Medical Centers based on their total cost; regional council overhead costs are allocated by FTE; and indirect costs are allocated to IP departments based on the approved step-down sequence and overhead rate calculations. This is intended to capture a fully costed final product or service that includes direct and indirect costs with consistency.
3	Cost Allocation Methodology	Assignment Methods (Direct Trace, Relational, General Allocation)	The system shall model costs based on various cost assignment methodologies (e.g., direct assignment, general allocation, cause and effect, etc.).	The system shall map costs to activities based on the mapping tables, DSSRVUs, feeder key, etc.
4	Cost Allocation Methodology	Costing Methodology	The system shall calculate and allocate costs based on financial system requirements and on a	The system shall allocate costs to adhere to the MCAO's timeline. Currently, all costs are allocated monthly.

I.D.	Category	Subcategory	Requirement	Requirement Description
			periodic basis (e.g., monthly cycle).	
5	Cost Allocation Methodology	Costing Methodology	The system shall allow activity drivers/weighting factors (e.g., DSSRVUs) and allocations to support calculations up to 8 decimal places.	The system shall support the VA's current logic where DSSRVUs are generated for each product with 4 decimal places but can allocate costs up to 8 decimal places.
6	Cost Allocation Methodology	Costing Methodology	The system shall support MCA methodologies defined in Statements of Federal Financial Accounting Standards (SSFAS) No. 4 [i.e., activity-based costing structure (pooling at the activity level) and job costing structure (pooling at the product level)].	The system's cost structure shall be configurable with federal accounting standards.
7	Cost Allocation Methodology	Costing Methodology	The system shall support full-cost calculation, to include direct and indirect costs, in accordance with SFFAS No. 4.	The system's full-cost computation shall be aligned with federal accounting standards where all costs that should be costed are costed.
8	Cost Allocation Methodology	Costing Methodology	The system shall load the prior year's actual cost data (e.g., supplies, exams, procedures, etc.) to use as the threshold levels for the upcoming fiscal year.	The system shall use the prior year's actuals as the threshold levels for the upcoming fiscal year, following the MCAO's current methodology.
9	Cost Allocation Methodology	Costing Methodology	The system shall dynamically model costs across various dimensions (e.g., patients, products, encounters, programs, departments, appropriations, etc.) for final cost objectives based on activity drivers.	The system needs to cost various final cost objectives including patients, products, encounters, programs, departments, appropriations, etc. per business needs and allocate their costs according to business rules. The system shall calculate product costs within each IP department based on DSSRVUs, product volume, and costs by cost type.

I.D.	Category	Subcategory	Requirement	Requirement Description
10	Cost Allocation Methodology	Costing Methodology	The system shall support the centralized management of the cost methodology and process and the publishing of model updates to the child cost models.	The system shall allow centralized, authorized users to maintain the cost methodology business rules - while allowing adjustments (as required) to be pushed to the child cost models (at VA Medical Centers). Additionally, the system must support the VA's current methodology where there are 133 child models that roll up to one parent model controlled by the MCAO.
11	Cost Model Allocation Execution	Allocation management	The system shall support business rules for when a new costed activity with no activity cost driver is added.	The system shall allow for the coding of both hard stops to halt modeling and thresholds to allow the model's processing to continue under business rules when new products without an assigned activity driver (e.g., DSSRVU) is added. The functionality can be adjusted as required.
12	Cost Model Allocation Execution	Cost Model Allocation Configuration	The system shall allow year-to-date (YTD) costing using current resource and activity drivers.	The accumulation of twelve months YTD costing is needed to facilitate the normalization/equalization (i.e., applying changes YTD) of costed results; thus, providing the ability to make adjustments to an activity driver value and have it reapplied to the prior periods for the fiscal year.
13	Cost Model Allocation Execution	Cost Model Allocation Configuration	The system shall support multiple cost driver types (e.g., percentage, fixed value, dynamic calculation, unit of measure, etc.).	The system shall support the identification of cost driver by type and category for each product.

I.D.	Category	Subcategory	Requirement	Requirement Description
14	Cost Model Allocation Execution	Model Scalability	The system shall support business rules that allow for the creation of new activities (e.g., products) and activity drivers (e.g., DSSRVUs) to be costed to scale to meet business needs.	The system shall handle the creation of any new products and their associated activity drivers as the need arises.
15	Cost Model Allocation Execution	Model validation	The system shall rerun, stop, or reset the cost modeling process if input data is refreshed or issues with the costing data has been determined.	The system shall rerun its analyses if input data is updated (e.g., after a VA Medical Center corrects an error). The system must reset the process to correct for errors found with the costing data.
16	Cost Model Inputs	Cost centers and cost activities	The system shall support the aggregation of costs by multiple dimensions (e.g., cost center, activities, activity drivers) for the purposes of cost modeling.	The system shall support the organization of costs into cost centers comparable to the current setup (cost centers, departments, etc.), and have the scalability to meet the future needs of the VA.
17	Cost Model Inputs	Data Ingestion / Transformation	The system shall reject data from source financial and operational systems' extracts based on business rules as part of ingestion.	The system shall block transactions from source financial systems from entering the system (e.g., payroll accrual amounts) in relation to withholding exempt costs from the costing process.
18	Cost Model Inputs	Data Ingestion / Transformation	The system shall be capable of ingesting common financial and operational data formats (e.g., .SQL, .CSV, .TXT, .SAS, etc.).	The system shall ingest industry leading financial data formats.
19	Cost Model Inputs	Data validation	The system shall support reporting throughout the cost allocation process to support validation, variance, reconciliation, auditing, and other ad-hoc analyses as required.	The system shall support reporting through various stages of the cost allocation process, including data validation, variance in thresholds (i.e., prior year's actuals) and actual data identification, data reconciliation between subsystems, etc.

I.D.	Category	Subcategory	Requirement	Requirement Description
20	Cost Model Inputs	Final cost objectives / services / products	The system must support business rules that allow for approximately 100,000 activities (e.g., IP) to be costed within the over 2,000 cost centers (e.g., department) across VA.	The system requires a high product limitation to eliminate the need to split up departments.
21	Cost Model Inputs	Cost centers and cost activities	The system shall support the creation of alphanumeric codes up to 20 digits to operate as keys to support the cost modeling process by categorizing groups of employees, job codes, and accounts.	VA's unique identifier feeder system has a selection of specific characteristics to create DSSRVUs relevant for capturing operational activities, activity units, and unit costs. This unique information is used in the cost allocation methodology and reporting. Feeder keys are the longest alphanumeric codes used by VA (20 digits).
22	Cost Model Outputs and Reporting	Business Intelligence	The system's costing capabilities shall allow for custom costed data extracts enabling users to conduct financial management, performance measurement, and cost accounting duties.	The system's costing methodology shall support data extracts that allow end users to conduct trend analysis and other performance metrics by various costing metrics (e.g., period, cost center, activities).
23	Cost Model Outputs and Reporting	Business Intelligence	The system shall ingest data to support reports to compare VA provided care with privately provided care (e.g., Community Care).	VA has a need to identify and compare VA care costs with care in the community cost (e.g., Current Procedural Terminology (CPT) codes) to better inform decisions for supplies and care provided.

I.D.	Category	Subcategory	Requirement	Requirement Description
24	Cost Model Outputs and Reporting	Output Validation	The system shall be capable of summarizing current month expenditures for selected financial records and deleting summarized records which have zero expenditures and create an output file with appropriate data fields based on business rules set forth by reporting segments (i.e., Veteran Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA)).	The system shall select criteria for VBA, VHA, and NCA Integrated Financial and Acquisition Management System (iFAMS) data based on Budget Object Code (BOC) and Division to segregate data appropriately and report on operations and operational costs.
25	Cost Model Outputs and Reporting	Reporting (User specific, standard such as Statement of Net Cost)	The system shall be capable of extracting data processed by the cost model in preparation for distribution of that data to end-users in a format defined by business rules.	The current MCA system outputs post-processed costing and operational data in extracts which are transformed and delivered through National Data Extracts (NDEs) to end-users for use in reporting and analytics needs.
26	Cost Model Outputs and Reporting	Reporting (User specific, standard such as Statement of Net Cost)	The system shall allow users to create and perform data queries and save queries for recurrent use.	The system shall allow users to filter ingested data through queries. Because of the nature of cost analysis, these specific queries can be saved for later use by the user.

I.D.	Category	Subcategory	Requirement	Requirement Description
27	Information and System	User Interface	The system shall perform scenario analyses to determine the impact of adjusting cost drivers and to support modeling functions for budgeting, strategic analyses, and competitive bidding so that a VA Medical Center can model changes in operational activity, cost, and reimbursement.	The Clinical Financial Planner (CFP) is a module of the DSS MCA that provides modeling functions for budgeting, strategic analyses, and competitive bidding. A hospital can model changes in clinical activity, cost, and reimbursement through CFP. Consequently, the system shall have modeling capabilities to meet the requirements of specific VA Medical Centers for analyzing changes to operations and costing. The system shall allow the MCAO and center teams to conduct what-if analyses to analyze the impact of changes to cost drivers, such as DSSRVUs.
28	Information and System	Availability Management	The system shall have a Recovery Point Objective (RPO) of 12 hours and a Recovery Time Objective (RTO) of 72 hours.	The system shall not lose more than 12 hours' worth of data and cannot be down for more than 72 hours to prevent negative impacts to MCAO's operations.
29	Information and System	Availability Management	The system shall have a remote disaster recovery site with required hardware and software, that is a minimum of 150 miles away from the primary site, and that can be tested yearly.	The system shall have a separate, identical environment significantly distanced from the production system to ensure continuity of operations in the event of a disaster and to meet compliance requirements.
30	Information and System	Availability Management	The system shall have a service availability of 99.5% uptime per year.	The system shall have 99.5% availability with no more than 43.8 hours of unplanned downtime per year.

I.D.	Category	Subcategory	Requirement	Requirement Description
31	Information and System	Backup Recovery	The system shall allow for weekly full application backups and daily incremental backups for application recovery in which backups shall be saved for a minimum of one month.	The system shall maintain regular data backups for all layers of the solution.
32	Information and System	Capacity Management	The system shall have the capacity to support at least 120 front-end concurrent users from the MCA office.	The system shall have sufficient capacity to support all the necessary front-end (i.e., users who may interact with the system but not make changes to core system functionality) and back-end users (i.e., users who interact with the system and may make changes to core system functionality) without negatively impacting system performance.
33	Information and System	Data	The system shall follow database naming standards utilizing VA and industry best practices, including but not limited to those utilized by Electronic Health Record Modernization (EHRM), FMS, iFAMS, and other data sources.	The system shall use the most efficient methods of naming standards for consistency across all layers of the system.
34	Information and System	Data	The system shall complete data validation functions for pre-processed data based on business rules to ensure data accuracy.	The system shall follow MCAO's direction and logic for preparing data before being processed by the DSS.
35	Information and System	Data	The system shall allow approved super users to make changes or data corrections either from the application or database.	The system shall allow for necessary configuration changes, updates, and upgrades by super users to maintain the DSS.

I.D.	Category	Subcategory	Requirement	Requirement Description
36	Information and System	Data	The system shall generate outbound data for post-production processing as a data extract in.CSV flat file formats to be stored and used for audit/quality validation and reporting purposes.	The system is dependent on the current VA Storage Area Network for data extract file storage and the MCAO Cost Reporting (DSR) is dependent on the flat file format for reporting capabilities that require data extracts.
37	Information and System	Data	The system shall ingest and migrate historical data or existing input data to the new system that enables a minimum of minus three-years trending of legacy 'analogous' reports.	The system shall migrate input data from the current solution to support thresholds, historical reports, spend analysis, YTD equalization, and other relevant business needs.
38	Information and System	Data	The system shall retain one year of pre-processed input data files from all data sources.	The system shall retain pre-processed data to ensure data recovery in the event of system downtime or failures and to meet audit requirements.
39	Information and System	Data	The system shall retain the previous three years of data (i.e., current year and two years prior on a rolling basis) costed by the model (e.g., staging and processed data) in the database.	The system shall retain data in accordance with VA data policies and to the extent needed to ensure sufficient recovery of data in the event of system downtime or system failure and to meet audit requirements.
40	Information and System	Data	The system shall accept direct data files and flat files from AITC for VHA National Database operational data and load that data into the system.	The system shall accept the files related to the VHA national database from the Austin Data Center as inbound files.
41	Information and System	Disaster Recovery	The system shall perform a minimum of weekly full system encrypted backups for disaster recovery to be stored onsite or at an alternate location for three years.	The system shall retain and encrypt data in accordance with VA data policies and to the extent needed to ensure sufficient recovery of data in the event of system downtime or failure and to meet audit requirements.

I.D.	Category	Subcategory	Requirement	Requirement Description
42	Information and System	Future State	The system shall send and receive data from future VA cloud and on-premises data sources for input and output destinations.	The system shall efficiently migrate to modern, cloud-based, and on-premises solutions as needed to adhere to federal mandates and MCAO leadership priorities.
43	Information and System	Future State	The system shall have the capability to obtain an Authority to Operate (ATO) and either be hosted on-premises or in a FedRamp moderate cloud solution.	The system shall comply with federal information technology (IT) mandates and Federal Information Security Controls Audit Manual (FISCAM) policies.
44	Information and System	Future State	The system shall be implemented and configured to allow for automation and/or machine learning processes to reduce the system cost and increase operational efficiency.	The system shall easily meet the current and future needs of the MCAO by allowing for modern IT capabilities such as automation, Robotic Process Automation (RPA), Artificial Intelligence (AI), and Machine Learning (ML).
45	Information and System	Infrastructure	The system shall have dedicated environments for Development, Patching, Testing, Training, User Acceptance, Production, and Disaster Recovery. The capacity for the Disaster Recovery environment should match 100% capacity of the production environment and 25-50% capacity of the remaining environments based on the business needs.	The system shall have separate and dedicated environments to meet the industry standard software development life cycle and MCAO user needs.
46	Information and System	Infrastructure	The system shall have the capability to utilize Application Programming Interfaces (APIs) or integrations, microservices, and service-oriented architecture based on current and future potential integration points (e.g.,	The system shall meet the current and future needs of the MCAO by allowing for modern IT capabilities such as API integration, microservices, and service-oriented architecture.

I.D.	Category	Subcategory	Requirement	Requirement Description
			Electronic Health Record Modernization (EHRM), iFAMS).	
47	Information and System	Infrastructure	The system shall have sufficient network infrastructure to receive all daily and monthly input data files from all current and future data sources without any errors during data transfers.	The system shall have enough capacity (e.g., network capacity, bandwidth, firewalls, etc.) to receive and process all data files without errors or failures.
48	Information and System	Maintainability	The system shall ensure that any changes made to the system by administrative users are properly logged.	The system shall update, upgrade, and patch without impacting users or creating significant system downtime.
49	Information and System	Maintainability	The solution vendor shall maintain the most recent and up to date documentation including but not limited to patch documentation and workflows.	The system or solution vendor shall generate documents to aid with system configurations and process documentation to allow for efficient and consistent implementation and change management in compliance with VA processes for use by stakeholders.
50	Information and System	Maintainability	The system shall have the capability to be upgraded and maintain previous baseline configurations in case of rollback (e.g., hardware, software, firmware, configuration files, etc.). The upgrade shall cause minimal downtime according to business rules with no loss of data or functionality after changes are implemented.	The system shall have its hardware and software upgraded as needed with little downtime and without losing any previously existing data or functionality that the VA may rely on.

I.D.	Category	Subcategory	Requirement	Requirement Description
51	Information and System	Maintainability	The system shall distribute code developed in a timely manner according to business rules to correct a major software bug (e.g., hot fixes) without downtime, user interruption, or loss of data.	The system shall deploy hot fixes without any system downtime or user impact.
52	Information and System	Software	The system shall have the capability for users to configure, customize, and bookmark commonly used views and reports to their account based on role, function, and/or location.	The system shall have a customizable user interface.
53	Information and System	Software	The system shall be accessible to users utilizing VA approved operating systems (e.g., Windows, Mac), browsers (e.g., Edge, Safari), and other solutions approved by the VA.	The system shall operate on VA approved IT software.
54	Information and System	Software	The system shall support installations on local machines and other platforms (e.g., web portals) to meet the current and future growth needs across the VA enterprise.	The system shall allow current and future users to operate and maintain the system.
55	Information and System	Software	The system shall have the capability to scale its infrastructure with growing needs such as additional data sources, centers, usage, or throughput.	The system shall meet the current and future needs of the MCAO by scaling the infrastructure accordingly.

I.D.	Category	Subcategory	Requirement	Requirement Description
56	Information and System	Software	The system shall allow Center users (e.g., MCA Site staff) to review their data once it is loaded into the database and run system reports to confirm the accuracy of their cost center's (e.g., center, VISN, department) data.	The system shall have the ability to allow front end users to review their center's data to validate the information after it has been input into the system and before the month end process begins
57	Information and System	Software	The system shall allow Center users (e.g., MCA Site staff) to schedule batch jobs on their center's pre-processed and processed data.	The system shall have the ability to allow users from VA Medical Centers to schedule system-run jobs to process their centers pre-processed and processed center data.
58	Information and System	Software	The system shall allow cost modelling users to set up and run Month End batch jobs to process prepared and validated data.	The system shall have the ability to allow users to execute all system-run costing jobs in sequence and without pause to complete the cost modeling processes
59	Information and System	Software	The system shall convert data source file inputs from .txt and delimited flat files into an easily accessible format of modern database engines.	The system shall convert inbound data files to an easily accessible format that modern database engine solutions will process.
60	Information and System	Software	The system shall edit, delete, concatenate, and compute fields in the processed data for financial and operational files.	The system shall perform data manipulations to input data files for data preparation before DSS processing steps begin.
61	Information and System	Software	The system shall accept new file types as inputs for data sources within the cost allocation process and scale to meet business needs.	The system shall accept input data files from new and existing data sources to be prepared and processed by the DSS solution.

I.D.	Category	Subcategory	Requirement	Requirement Description
62	Information and System	Software	The system shall meet all requirements outlined within VA Technical Reference Model (TRM) before installing on-premises or cloud, which includes completing a Content Request Form for the required assessment found on trm.oit.va.gov .	Any new system technology shall successfully complete the VA approval process using the VA TRM.
63	Information and System	Software	The system shall only use commonly supported programming languages with readily available documentation and resources.	The system shall only use widely supported technologies to protect the VA from unnecessary costs, vulnerabilities, or resource constraints.
64	Information and System	Software	The system shall be compliant with Section 508 of the Rehabilitation Act of 1973.	All government applications must be compliant with Section 508 of the Rehabilitation Act of 1973.
65	Information and System	Software	The system shall possess the ability to provide self-service capabilities within the system for frequently asked questions (FAQ) and common issues encountered by users.	There should be a capability to assist users with frequently asked questions or frequently encountered issues to help them efficiently solve some common day to day issues quickly without needing to engage higher level tech support resources or create tickets.
66	Information and System	Software	The system shall have the capacity for one-year pre-processed input data, three years of database data, three years of data extracts for post-processing, and scale storage capacity for future needs. The current storage capacity is 22 TB for database data and 5 TB for the post-processing files.	The system shall store all active process data, all required retention data, and scale for future requirements.

I.D.	Category	Subcategory	Requirement	Requirement Description
67	Information and System	System Interface	The system shall accept and read flat file inputs and financial data from two source systems [Health Resources Priority and Allocation System (HR PAS) and Personnel and Accounting Integrated Data (PAID)].	The system shall read and accept the current output data files from the HR PAS and PAID systems as inputs into the DSS.
68	Information and System	System Interface	The system shall accept and read flat file or physical sequential file inputs for financial and operational data received from different ancillary data sources (currently 15 ancillary data source feeds are received).	The system shall read and accept the current output data files from ancillary data source systems as inputs into the DSS.
69	Information and System	System Interface	The system shall accept and read mainframe Mailman message files received from medical operational systems Veterans Information System and Technology Architecture (Vista) and convert medical operational data grouped by fiscal year and month for processing by the cost model solution.	The system shall read and accept the current output data from the Vista system as inputs into the DSS.
70	Information and System	System Interface	The system shall be able to accept and read American Standard Code for Information Interchange (ASCII)-encoded text file inputs with financial data from two financial system sources (Financial Management Systems (FMS) and iFAMS).	The system shall read and accept the current output data from the VA's financial record system as inputs into the DSS.

I.D.	Category	Subcategory	Requirement	Requirement Description
71	Information and System	System Interface	The system shall complete required data preparation, conversion, and feeding of data into the database daily in preparation for the cost allocation process.	The system shall take the necessary steps required to load the data into the correct locations in the database from all inbound data files.
72	Information and System	System Performance	The system shall ingest a minimum 130 million data points monthly to execute the cost modeling process.	The system shall perform at the current processing capacity of at least 130 million data points monthly.
73	Information and System	System Performance	The system shall store a minimum of 400 activities cost drivers (e.g., labor, supply, and contract labor mapping) from three fiscal years (current year and prior two years).	The system shall store at minimum 400 cost drivers with the ability to scale as system needs grow.
74	Information and System	System Performance	The system shall have sufficient network infrastructure to send all monthly data extract files of at least 29GB per month, without network errors or slowdowns.	The system shall have enough capacity (network capacity, bandwidth, firewalls, etc.) to send all data files without errors or failures.
75	Information and System	System Performance	The system shall complete cost model (financial and operational) processing jobs outside of core business hours (8:00 CST to 16:00 CST).	The system shall run cost model processing jobs overnight and not be limited to weekends to complete jobs so that business operations are not impacted.
76	Information and System	User Interface	The system shall have the functionality for remote configuration by technology administrators and super users.	The user population is spread across the U.S. and the system's users need to be able access and configure the system remotely.

I.D.	Category	Subcategory	Requirement	Requirement Description
77	Information and System	User Interface	The system shall have the capability to utilize alerts and notifications to communicate with users for a variety of notifications, including when previously queued tasks like inbound or outbound extracts are started, completed, or if they fail.	The system should send notifications and alerts to communicate with users and notify them when their job/task starts/completes.
78	Information and System	User Interface	The system shall provide a consistent user interface, menus, and commands across all parts of the solution to provide users with a consistent and efficient system experience.	The system shall have a functionally and visually consistent or unified (user interface/user experience) UI/UX such as having the same sized objects, colors, and fields.
79	Information and System	User Interface	The system shall produce error messages that can clearly identify problems or system issues.	In the case that the system encounters an error, it should produce an error message with appropriate verbiage or a code that identifies an issue and possible solution.
80	Information and System	User Interface	The system vendor shall provide fully searchable, indexed, and comprehensive solution manuals, documentation, workflows, training, and user-help capabilities within the system to support to all user functions.	All solutions should provide documentation, manuals, and training materials that are able to be easily located and are searchable.
81	Information and System	Vendor	The system vendor shall provide expertise on technical components of the solution.	The vendor should have resources that understand the technical underpinnings of the solution and should be available to support should an issue arise.

I.D.	Category	Subcategory	Requirement	Requirement Description
82	Governance and Operating Model	Audit and Accountability	The system shall support auditing functions by allowing the following: - Auditing and alerting of defined events captured by timestamp, user account, location, and nature of the event. - Generating on-demand ad hoc audits. - Access to audit reports. - Integration of audit and scanning activities.	The system shall: • Include automated ability to identify significant security events (per "VA Security Event and Suspicious Behavior Definitions List - 9/14/2015") based on the location, time, person (for non-repudiation all activities must be logged by an account name), or other criteria established by the International Organization for Standardization (ISO). • Have flexible audit levels that can be changed based on updated risks by credible sources (law enforcement, security agencies). • Provide alerts for automated audit functions or logging encounter failures. Additional criteria for alerts can be established by the ISO. • Access to audit records is restricted from unauthorized sources through the use of VA approved mechanisms. • The system shall allow for integration of audit and scanning activities, should they intersect. Logistical: • Audits must be performed monthly, at a minimum, or immediately for security related events.

I.D.	Category	Subcategory	Requirement	Requirement Description
83	Governance and Operating Model	Audit and Accountability	The system shall manage, store and allow for ad hoc reporting from files used for audit (e.g., logs and error reports) to support audit trails and after-the-fact investigations of security incidents, as well as meet regulatory and retention requirements, which include: - Six years for a security breach, - Five years for Intelligence Information or financial records, and - One year for the national archives and records administration or, as stated by the legislation, whichever is greater.	The system shall: • Allow for retention of audit records for a minimum of six (6) years for logs that describe a security breach, five (5) years for Sources and Methods Intelligence Information (SAMI) or financial records, and one (1) year or as documented in the National Archives and Records Administration (NARA) retention periods, Health Insurance Portability and Accountability Act of 1996 (HIPAA) legislation (for VHA), whichever is greater. • Have sufficient storage volume to ensure retention of audit files are kept for the defined time period. Audit records shall be centralized in the VA Central Data Lake, per Office of Management and Budget (OMB) 21-31, for management and configuration purposes. • Compile audit records into a system-wide audit trail that can be organized by criteria such as time stamp, user, condition, severity, access to PII, etc.
84	Cost Allocation Methodology	Costing Methodology	The system shall validate the cost allocation sequence assigned to each costing segment and cost center.	Ability to run reports to verify that all indirect costs have passed to its assigned departments (no dead-end costs) and no variable indirect cost is present. Ability to run reports to validate the order number sequence assigned to each department in the cost accounting module for review and auditing purposes.

I.D.	Category	Subcategory	Requirement	Requirement Description
85	Cost Model Allocation Execution	Cost Model Allocation Configuration	The system shall be able to validate the number of departments and their assigned sub-departments based on the cost allocation structure.	Ability to validate the number of the departments and its sub-departments (i.e., parent/child assignments), ensuring that the number of sub-departments assigned to each department is correct.
86	Governance and Operating Model	Business Process	The system shall encrypt data at rest and manage and monitor master data to ensure validity and integrity.	The system shall: • Ensure master data records are valid, complete, accurate, contain no duplicates. • Monitor any changes to master data. • Protect master data confidentiality, as needed. • Ensure data is encrypted at rest and is only accessible by authorized personnel or per business rules.

I.D.	Category	Subcategory	Requirement	Requirement Description
87	Governance and Operating Model	Risk Assessment	The system shall run routine security scanning tools for vulnerabilities in the information system and identify and report potential vulnerabilities affecting the system per the business assessment risk.	The system shall allow for any of the applicable security scans below to be run, at a minimum, in the timeframes below, ad hoc when major changes take place, or when new vulnerabilities are detected: -Nessus – Monthly -Security Configuration Compliance Data (SCCD) – Quarterly -Pen Test, Web Application Security Assessment (WASA), Mobile Application Security Assessment (MASA), Application Threat Model, Application Security Test (the latter two are code and design reviews) – annually Logistical: Coordination for scan requirements (ports to remain open, service accounts for logging in, etc.) is done with Cybersecurity Operations Center (CSOC) or with any third party entities that might run comparable scans (in which case the scans need to be accepted by CSOC to meet their requirements).

I.D.	Category	Subcategory	Requirement	Requirement Description
88	Governance and Operating Model	Transparency	The system shall provide a privacy notice when personal information/personal health information (PII/PHI) is being accessed. The notice shall describe the nature of the PII, why it is being collected, how it is being guarded, and how it is being used. PII/PHI shall not be editable for corrections. If corrections are needed, the PII/PHI will need to be re-sent from the source.	The system shall provide a privacy notice when PII/PHI is being accessed electronically, that describes the nature of the information being collected, authority for collecting it, safeguarding of the information, and how the PII is being used. This can be done through documentation.
89	Governance and Operating Model	Cost Accounting Policy	The system shall support the cost methodology procedures per the MCA policy to accumulate, monitor, and report costs consistently and routinely for management information purposes.	The system shall have the: • Ability to support the cost methodology procedures to accumulate and report costs continuously, routinely, and consistently for management information purposes that meets its internal goals. • Ability to support each reporting entity to accumulate, monitor, and report the costs of its activities regularly for management information purposes. Costs may be accumulated either through cost accounting systems or cost-finding techniques according to management needs and external reporting measures. • Ability to perform the cost assignments using the following methods listed in the order of preference: (a) directly tracing costs wherever feasible and economically practicable. (b) assigning costs on a cause-and-

I.D.	Category	Subcategory	Requirement	Requirement Description
				effect basis, or (c) allocating costs reasonably and consistently.

I.D.	Category	Subcategory	Requirement	Requirement Description
90	Governance and Operating Model	Internal Audit & Internal Controls	The system shall compare the data input entered during the ingestion process to the data output or to the standard factors driven by historical data to identify fluctuations, inconsistencies, and trends based on defined business rules (such as standard deviation).	The system shall have the: • Ability to use the feeder systems (i.e., Vista/EHRM) routine (Fileman) to pull all encounters and compare them to the prior fiscal period to identify volume spikes and dips that may indicate deficiencies and inconsistencies. • Ability to reconcile Laboratory Blood Bank (LBB) extracted data to the source data to ensure the data that have been extracted are accurate and complete • Ability to reconcile the input data from the feeder systems (i.e., Vista/EHRM) to the ALB output data for accuracy and completeness. • Ability to compare the totals for each ward from the Admission extract file to the Gains and Losses (G&L) source data to ensure the data and recorded records are consistent and captured accurately and completely.

I.D.	Category	Subcategory	Requirement	Requirement Description
91	Governance and Operating Model	Internal Audit & Internal Controls	The system shall provide capability for data validation and edit checks to resolve data allocation issues, such as when data is duplicated, missing, or deemed insufficient.	The system shall have the: • Ability to identify common mistakes (e.g., Incorrect department and Account Level Budgeter Cost Center (ALBCC)) in ALB before moving the data to DCM. • Ability to identify variances between the cost reports to ensure that data are processed completely in the cost accounting module. • Ability to identify variances in cost and volumes between the mainframe and NDE. • Ability to run pre-extract audits from the feeder system (i.e., Vista/EHRM) before running monthly extracts to identify unusual volume reports, unusual cost reports, identifiers, and clinic reports. • Ability to support the data integrity, reconciliation, and standardization audits around the data input - source data, and data outputs - NDE.

I.D.	Category	Subcategory	Requirement	Requirement Description
92	Governance and Operating Model	Internal Audit & Internal Controls	The system shall support periodic reconciliations and reconciliation trails and provide validation capabilities of cost data throughout the cost preparation and cost modeling processes.	The system shall have the ability to fully integrate with other VHA systems to provide an audit trail that traces the transaction from the original cost pool to the final cost object. The system shall have the ability to support reconciliation and certification to ensure that all costs from the general ledger operating accounts are reconciled to the data contained in the system.
93	Governance and Operating Model	Internal Audit & Internal Controls	The system shall produce and maintain a log that captures data changes resulting from errors and inconsistencies made during the cost modeling process.	The system shall have the ability to produce and maintain a log that captures the audit findings, errors, and changes. The log will need to capture all related relevant information to each item reported in the log, including the file name, date and time, the type of error or finding, and the impact of the error or finding. The system shall have the ability to process common errors and generate model rules. If the error is significant (e.g., system crash), it needs to produce a report showing where the error is or what the issue is.

I.D.	Category	Subcategory	Requirement	Requirement Description
94	Governance and Operating Model	Internal Audit & Internal Controls	The system shall have the capability to archive seven years of historical data and generate reports showing data inconsistencies based on defined business rules.	The system shall have the ability to allow the MCAO to conduct outlier analysis, one of the key methods used to identify variances or issues with model inputs or processing. The system shall have the ability to compare historical data to current data to report on outliers for inconsistencies within the data reported in the system for advanced analytics use cases.
95	Governance and Operating Model	Internal Audit & Internal Controls	The system shall restrict the ability to remove, overwrite, or reallocate costing activity and its related activity drivers based on defined business rules and established account privileges.	The system shall have the ability to restrict users from deleting, overwriting, or moving a product that has actual volumes (in product volume (PRODVOL) or change detail (CHGDTL)) in the current fiscal year. The system shall have the ability to restrict users based on their user type or privileges to edit, overnight, or remove data in the system. Logistical: • Access requests must be processed only when initiated via written request from the user's management since they have adequate knowledge regarding the user's legitimate need to access/modify data. • The written or email request must provide the user's name and explicitly detail the access privileges requested. • User account request documentation must be completed in full prior to account

I.D.	Category	Subcategory	Requirement	Requirement Description
				creation. • If the request is received via email, the request must be verbally confirmed with the requester prior to granting access privileges, and the email must be printed and annotated with the date and time of the verbal verification. • Creation of user accounts or assignment of access privileges without the approved written or verified email request is forbidden. Per VA Directive 6517 (Cloud Systems), NIST 800-53, 5 U.S.C. Section: 552a(e)(9); OMB M-06-16; OMB M-07-16 ,Att. 1, A.2.d. – • Allow for access to certain system entities (files, records, domains, etc.) based on access control lists/policies. • Allow for restrictions on access based on account type (i.e.: set times of day access is allowed, duration of access, etc.). • Enable assignment of the least amount of functions needed for a particular user role to do their duties, based on role scheme. • Prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards. • Restrict access to data repositories containing organization-defined information types. • Ensure that application data and reports and other output are

I.D.	Category	Subcategory	Requirement	Requirement Description
				protected against unauthorized access.
96	Governance and Operating Model	Internal Audit & Internal Controls	The system shall retain automated notification transmittals for audit review.	The system shall have the ability to support the review of any warnings or error messages to ensure that all costs are completely processed for all fiscal periods to date. The system shall have the ability to send a notification to/from the national and VA Medical Center level for any identified audit errors, issues, variances, and data inconsistencies.
97	Governance and Operating Model	Internal Audit & Internal Controls	The system shall report on identified rejected data and error messages through the ingestion, cost preparation, and cost modeling.	The system shall have the ability to run pre-extract audits from the feeder system (e.g., Vista/EHRM) and monthly extracts audit to identify unusual data or errors.
98	Governance and Operating Model	Internal Audit & Internal Controls	The system shall provide auditing capabilities to retain data characteristics from source systems and have a high degree of traceability and transparency throughout the cost modeling process.	The system shall trace the costs throughout the entire cost modeling process, from their input to the final cost objectives.
99	Governance and Operating Model	Internal Audit & Internal Controls	The system shall report on identified incorrect and duplicate cost data and products entered during the ingestion process per defined business rules.	The system shall have the ability to identify duplicate products and costs in the different departments to validate that there are no unintentional duplicate products and that the correct number of duplicates exists in the appropriate departments.

I.D.	Category	Subcategory	Requirement	Requirement Description
100	Information and System	Access Control	The system shall provide, monitor, and manage standard, privileged, service, shared, group, temporary, and emergency accounts to have unique permissions, including uploading, downloading, and editing data under the role-based access scheme.	The system shall: • Support applicable types of users (standard, privileges, service, group, etc.) for the system and have individual permissions for each role. • Establish usage restrictions (uploading/downloading data, editing data, etc.), and configuration based on account types. • Enable logging for identification of atypical usage, ensure permissions are accurate and accounts are active. • Allow for immediate disabling of accounts when they are identified as a significant risk. Definition of significant risk and how that risk is discovered is established by the ISO in system policy. "Immediate" disabling is VA defined. • Terminate shared/group account credentials when users leave the group.

I.D.	Category	Subcategory	Requirement	Requirement Description
101	Information and System	Access Control	The system shall allow response to automated or manual user account changes such as create, enable, modify, disable, move inactive, mark temporary, and create emergency information system accounts with notifications per business rules.	The system shall be able to: • Use automated or manual functions to create accounts if the system allows for creation of its own accounts (as opposed to using Active Directory (AD) or NMEA accounts). • Implement automatic or manual removal of inactive, temporary, or emergency accounts. • Enable logging or reporting to support auditing of account actions (creation, modification, disabling, etc.). • Notify specified system personnel regarding audits. • Allow for account termination and prompt revocation
102	Information and System	Access Control	The system shall enforce user-based roles to support the separation of duties based on security configuration for all user types.	The system shall: • Allow for separation of duties by allowing access based on user role for all user types. • Enforce approved authorizations to support separation of duties.

I.D.	Category	Subcategory	Requirement	Requirement Description
103	Information and System	Access Control	The system shall manage access to system entities (files, records, domains, etc.) based on the account type and roles (e.g., preventing least privileged accounts/roles from executing privileged accounts/roles capabilities).	The system shall: • Allow for access to certain system entities (files, records, domains, etc.) based on access control lists/policies. • Allow for restrictions on access based on account type (e.g., set times of day access is allowed, duration of access, etc.). • Enable assignment of the least amount of functions needed for a particular user role to do their duties, based on role scheme. • Prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards. • Restrict access to data repositories containing organization-defined information types. • Ensure that application data and reports and other output are protected against unauthorized access. Logistical: • Contractor and Service Account policy will be noted in contracts (required per control AC-2).
104	Information and System	Access Control	The system shall isolate security and system management functions from user functions by segregating CPUs, operating systems, addresses, or virtualization.	The system shall separate system management-related functionality from user functionality by using different central processing units, different instances of operating systems, virtualization techniques, or combination of these or other methods, as appropriate.

I.D.	Category	Subcategory	Requirement	Requirement Description
105	Information and System	Access Control	The system shall have safeguards and management flow processes to prevent information disclosure during transmission to interconnected systems.	The system shall: • Have safeguards in place to prevent disclosure of information during transmission to interconnected systems. • Allow for filtering of information (i.e., information contains PII or not) to determine how that information is allowed to flow (can be shared internally, externally, or both). • Pre-screen incoming information to ensure the validity of the information and ensure it comes from an authorized source.
106	Information and System	Access Control	The system shall manage sessions by allowing session lock or logout due to inactivity or timeout function and shall recognize and notify security violations and activities, including failed login attempts defined by business rules.	The system shall: • Allow for session lock or logout due to inactivity and have a timeout function. • Set the number of consecutive failed logins before either locking the account or preventing another login for a defined time. • Restrict the number of concurrent sessions any user or role can have running. • Display a public image when a session is locked and ensure the previous screen and PII are not viewable until the user logs back in. • Recognize and notify defined personnel of security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity.

I.D.	Category	Subcategory	Requirement	Requirement Description
107	Information and System	Access Control	The system shall allow for notifications upon logging into the system to perform the following: - Government system, consent to monitoring, penalties for unauthorized use, and privacy notices, - Appropriate warning banners are displayed before logging onto a system, and - Previous logon notification, including the date and time of the last logon and unsuccessful logins.	The system shall provide the following notifications upon logging into the system: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording.
108	Information and System	Access Control	The system shall allow for remote access that can be appropriately controlled, monitored, and protected to validate appropriate access for remote users.	The system shall: • Restrict the functions of remote users when they are using the system. • Immediately disconnect remote sessions if unauthorized activity is discovered. Logistical: • Remote usage will be monitored on various types of system components to help facilitate detection of cyber-attacks.

I.D.	Category	Subcategory	Requirement	Requirement Description
109	Information and System	Access Control	The system shall establish a trusted communications path between the user and the security functionality of the system; this includes entities that connect outside of the system boundaries.	The system shall: • Establish trust relationships for entities that connect to it outside of the system boundary (e.g., personal laptops, smartphones, tablets, etc.) to include if any system data is authorized to be stored on such entities. • Restrict use of organizationally trusted devices on external systems. • Prevent the unintended and unauthorized information transfer between system devices.
110	Governance and Operating Model	Regulatory Requirements	The system shall have mechanisms for validating that the data has been processed within the required timeframe based on the organization calendar to meet the applicable reporting requirements for external parties.	The system shall have the ability to provide confirmation that data was processed within the required time period to follow the VA's calendar and meet applicable reporting requirements of external bodies.

I.D.	Category	Subcategory	Requirement	Requirement Description
111	Governance and Operating Model	Risk Assessment	The system shall identify if the required data attributes entered during the ingestion process are negative, missing, inaccurate, or incomplete by applying defined business rules.	The system shall have the: • Ability to identify incomplete records from the feeder system (i.e., Vista/EHRM) to ensure all Event Capture records have patient or procedure information. • Ability to identify unusual prostatic costs, pharmacy volumes, costs attribute, missing data, or unusual volumes in the surgery file from the feeder systems (i.e., Vista/EHRM) as determined by a user-defined threshold value (i.e., cost or volume of a transaction is greater than the threshold value). • Ability to validate the Data Report from the feeder system (i.e., Vista/EHRM) to ensure no errors exist for medical record processing by verifying feeder systems extract counts are correct and Non-feeder systems extracts are present and reasonable. • Ability to use the Laboratory Blood Extract to identify potential errors from the feeder systems in the blood bank records, including the following attributes: transfusion date outside of the month (or year), incorrect number of units for a patient, and inaccurate or incomplete list of patients that have received transfusions.

I.D.	Category	Subcategory	Requirement	Requirement Description
112	Governance and Operating Model	Risk Assessment	The system shall identify cost center attribute inconsistencies based on the cost center activity drivers as per defined business rules.	The system shall have the ability to identify variances between different cost reports to ensure that data are processed completely and accurately in the Cost Accounting Module (CAM). The system shall have the ability to identify any new inconsistencies within the cost center attributes or job code levels for threshold and reporting purposes.
113	Information and System	Security Assessment and Authorization	The system shall authorize connections to organizational information systems and approved external systems.	The system shall: • Allow for interconnections with outside entities through use of Interconnection Security Agreement (ISA) / Memorandum of Understanding or Agreement (MOUs). • Authorize connections to organizational information systems and related components to include mobile devices, printers, servers, etc. through ISAs, Information Connection Document, or an Authority to Connect document. Logistical: Each ISA/MOU will document the characteristics of the connection, security requirements, and the nature of the information to be shared. It is required to be reviewed annually.

I.D.	Category	Subcategory	Requirement	Requirement Description
114	Information and System	Configuration Management	The system shall monitor and report on baseline configuration changes in an unauthorized manner and retain baseline configurations of the information system, including previous baseline configurations for rollbacks.	The system shall: • Include automated tools to help maintain baseline configurations for the system. Examples include inventory tools, configuration management, and network tools. These will track things like version numbers, patch levels, types of software being used, etc. • Allow for alerting to defined personnel when unauthorized configuration changes are implemented. • Maintain previous baseline configurations (hardware, software, firmware, configuration files and configuration records) in case of rollback. • Verify security functions to ensure any configuration changes do not affect the functions and that changes are working as designed.
115	Information and System	Configuration Management	The system shall prohibit the execution of non-local technologies based on a deny-all/employ-by-exception policy and shall track software licensing and generate error report for audit purposes.	The system shall: • Not allow for execution of non-local technologies as defined by the ISO (some definitions are provided at the VA level, through prohibited software/TRM). • Employ a deny-all/employ by exception policy to execution of unauthorized software (based on VA TRM). • The system shall track and manage software licensing, if applicable, to help with managing of software usage restrictions.

I.D.	Category	Subcategory	Requirement	Requirement Description
116	Information and System	Configuration Management	The system shall allow for port management that ensures essential capabilities are enabled such as sending and receiving data via Secure File Transfer Protocol (SFTP) and other VA approved secure file transfer protocols.	The system shall allow for port management that ensures only essential capabilities are enabled in the system. Examples can include Voice-over-IP (VOIP), security scans, file sharing (ex. File Transfer Protocol (FTP)), Hypertext Transfer Protocol (HTTP), Instant Messaging, USB restrictions, etc.
117	Information and System	Configuration Management	The system shall automate the management of system components and generate reports to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	The system shall provide automated tools and/or reports to create and maintain information system hardware inventories in the VA Governance, Risk, and Compliance software (serial number, model, device type, etc.), especially for virtual hardware.
118	Information and System	Identification and Authorization	The system shall implement multi-factor authentication for network access to privileged accounts, ensuring integration with AD.	The system shall: • Use multi-factor authentication (by Personal Identity Verification (PIV) and another method) for use of privileged accounts for system administration and non-privileged accounts for logging into the system. • Integrate with AD for front and back-end users. • Ensure one method of authentication is separate from the system login.
119	Information and System	Identification and Authorization	The system shall enforce minimum password complexity of requirements for case sensitivity, number of characters, a mix of upper-case letters, lower-case letters, numbers, and special characters.	The system shall enforce password complexity to include the number of upper- and lower-case characters, numbers, special characters, and length requirements; it shall also specify mandatory character changes, lifetime restrictions, and reuse rules.

I.D.	Category	Subcategory	Requirement	Requirement Description
120	Information and System	Identification and Authorization	The system shall ensure mapping for Public Key Infrastructure (PKI) certificates matches an authorized user before allowing access to the system.	The system shall ensure mapping for PKI certificates match to an authorized user of the system before allowing access to the system.
121	Information and System	Media Protection	The system shall restrict access to digital media and implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	The system shall: • Restrict use of digital media (flash drives, removable hard drives, magnetic tapes, CD, diskette, etc.). • Allow for cryptographic mechanisms to protect information on digital media that is removed from the system.
122	Governance and Operating Model	Risk Assessment	The system shall produce reports to perform risk and uncertainty analysis periodically over cost and cost activity.	The system shall have the ability to analyze the total and actual cost that has been reported in the system to show any inconsistencies. The system shall have the ability to perform risk analysis over the costs compared to VHA to VHA or VHA vs. Care in the Community (CITC).
123	Information and System	System and Communications Protection	The system shall implement security safeguards that protect the information system against, or limit the effects of, denial of service attacks using authorized security software.	The system shall implement security safeguards that protect the information system against, or limit the effects of, denial of service attacks using authorized security software such as IBM Security QRadar, Threat Radar, Cisco ASA FirePOWER, Mandiant FireEye services, SolarWinds Orion, NetScout, and Splunk.

I.D.	Category	Subcategory	Requirement	Requirement Description
124	Information and System	System and Communications Protection	The system shall manage and monitor communications with external sources within the system's boundaries.	The system shall: • Monitor and control communications at the system boundary and at key internal boundaries (i.e., incoming data, information transferred between key components). • Ensure there is a secure connection (e.g., handshake) between input and processing systems to ensure data is not lost. • Establish physical or logical separation of Implement subnetworks for publicly available system components and monitor open source (social media and other sites) information for evidence of unauthorized disclosure.
125	Information and System	System and Communications Protection	The system shall manage device network communications traffic by default, detect outgoing communications traffic posing a threat, monitor inbound and outbound communications traffic, and allow network communications traffic by exceptions based on business rules.	The system shall: • Use automated mechanisms to implement boundary protection and limit the number of external network connections to only those which are necessary for the operation of the system and scanning activities. • Have a unique managed interface for telecommunications devices that controls and protects the traffic flow between the system and the device. • Implement deny-all/allow by exception security for communications at managed interfaces. • Deny any external device using “split tunneling” (establishing non-remote access to the system while simultaneously being connected to an external source like printers).

I.D.	Category	Subcategory	Requirement	Requirement Description
126	Information and System	System and Communications Protection	The system shall use authenticated proxy servers and spam protection when communicating with external systems or devices to facilitate the protection of the information that is being transmitted.	The system shall: • Use proxy servers when defined internal communications are routed to external entities through managed interfaces. • Implement cryptographic mechanisms to ensure protection from disclosure of communications to unauthorized entities and ensure the information remains intact.
127	Information and System	System and Communications Protection	The system shall automatically terminate network connections associated with a communication session at the end of the session or after inactivity and if suspicious events occur.	The system shall terminate network connections used for communications sessions when that session ends or after a defined period of inactivity (NOTE: this is not the same as a session lock). The time period is VA defined as five minutes or less.
128	Information and System	System and Communications Protection	The system shall restrict mobile code technologies such as Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.	The system shall restrict use of mobile code to include (but not limited to) Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.
129	Information and System	System and Communications Protection	The system shall maintain separate execution domains for each execution process.	The system shall maintain separate execution domains for each executing process by assigning each process a separate address space. This ensures one process cannot control or modify another process without a security function.
130	Information and System	System and Information Integrity	The system shall generate error messages that provide general information for corrective actions without revealing information that could be exploited.	The system shall generate error messages that provide the information necessary for the corrective action but does not divulge information that can be exploited by adversaries.

I.D.	Category	Subcategory	Requirement	Requirement Description
131	Governance and Operating Model	Segregation of Duties	The system shall define and designate responsibility segments based on organizational structure and responsibilities per business rules.	The system shall have the ability to establish and designate responsibility segments based on organizational structure, responsibilities/missions, outputs, and budget accounts/funding authorities.
132	Cost Model Inputs	Final cost objectives / services / products	The system shall run month-end costing (financial and operational) activities (e.g., allocating costs to patients, products, encounters each month) in three business days after all inbound data is received to meet the business' needs.	The system shall produce cost outputs as defined by business rules for distribution to MCAO stakeholders for dissemination of cost information for individual business needs.
133	Cost Model Inputs	Data Ingestion / Transformation	The system shall be able to retrieve and transform data per the business rules (e.g., creating new columns, appending data, transforming data, generating computations (such as deriving cost driver percentages)).	The system shall be able to transform data from various data sources and append that data for ingestion into the cost model solution.
134	Governance and Operating Model	Regulatory Requirements	The system shall be compliant with the Health Insurance Portability and Accountability Act (HIPAA) of 1996.	The system must be compliant with HIPAA by having necessary access controls to prevent misuse of PHI, capability to enable end to end encryption for data both at rest and in-transit, activity monitoring, emergency measures such as backups and breach notifications, and physical storage security. This can be satisfied with a bolt-on solution if needed.

I.D.	Category	Subcategory	Requirement	Requirement Description
135	Information and System	Data	The system shall ingest and migrate historic model activities, activity drivers, and cost centers logic to enable a minimum of minus three-years trending of legacy 'analogous' reports.	The system shall migrate historic model activities, activity drivers, and cost centers logic from the current solution to support thresholds, historical reports, spend analysis, YTD equalization, and other relevant business needs.
136	Governance and Operating Model	Internal Audit & Internal Controls	The system shall allow for additional attributes/metadata to support financial, operational, and performance reporting supported by any data used for resource and activity allocation maintained through the modeling process.	Federal cost accounting often requires the capture of source and type of funding and relevant congressional Acts in order to provide reconciliation reports as required for compliance.
137	Governance and Operating Model	Internal Audit & Internal Controls	The system shall prevent incorrect and duplicate cost data and products from entering the system during the ingestion process per defined business rules.	The system shall have the ability to prevent duplicate products and costs in different departments from entering the system to prevent unintentional duplicate products from skewing the cost modeling process.
138	Cost Model Allocation Execution	Cost Model Allocation Configuration	The system shall support the capability to dynamically derive cost allocations using ingested data to be allocated to cost objectives based on defined business rules	VA's MCA dynamically calculates allocations based on pooled costs (MCA departments) and calculates the costs into individual products mapped to the department relevant to the cost center for allocation (e.g., meals in pooled cost (MCA department) are broken into individual meals based on patient stay to distribute the costs to a patient encounter).

I.D.	Category	Subcategory	Requirement	Requirement Description
139	Cost Model Allocation Execution	Cost Model Allocation Configuration	The system shall support the capability to derive dynamic cost drivers using ingested data to be used in cost allocations.	VA's MCA dynamically calculates drivers to allocate cost based on operational data (e.g., patient stay to derive "bed days"). These drivers are used in various cost allocations, including dynamically determined cost allocations pools.
140	Cost Model Allocation Execution	Cost Model Allocation Configuration	The system shall maintain, at minimum, 1 year of dynamically derived cost allocations and cost drivers.	VA's current system maintains dynamically calculated cost allocations and cost drivers in the MCA for 1 year before they are archived and exported for integration into NDEs. NDEs are created monthly based on year-to-date calculated cost allocations.