

Department of Veterans Affairs

Direct Secure Messaging Enhancements

Increments 1 and 2

Requirements Specification Document (RSD)



August 2015

Version 1.0

Revision History

Note: The revision history cycle begins once changes or enhancements are requested after the Requirements Specification Document has been base lined.

| Date | Version | Description | Author |
|------------|---------|--|---|
| 08/05/2015 | 1.0 | Finalized RSD for increments 1 and 2 and distributed for signature | Direct Secure Messaging Enhancements PMO and Development Team |
| 07/31/2015 | 0.3 | Updated RSD to include Increment 1 and 2 information | Direct Secure Messaging Enhancements PMO and Development Team |
| 05/05/2015 | 0.2 | Final MS 1 for Provisioning for signature | Direct Secure Messaging Enhancements PMO Team |
| 04/14/2015 | 0.1 | Initial draft for Direct Secure Messaging Enhancements project | Direct Secure Messaging Enhancements PMO Team |

Table of Contents

| | |
|---|-----------|
| 1. Introduction | 1 |
| 1.1. Purpose | 1 |
| 1.2. Scope | 2 |
| 1.3. References | 2 |
| 2. Overall Description | 3 |
| 2.1. Accessibility Specifications..... | 3 |
| 2.2. Business Rules Specification..... | 3 |
| 2.3. Design Constraints Specification..... | 3 |
| 2.4. Disaster Recovery Specification | 4 |
| 2.5. Documentation Specifications | 4 |
| 2.6. Functional Specifications | 4 |
| 2.7. User Interface (GUI) Specifications | 10 |
| 2.8. Multi-divisional Specifications | 11 |
| 2.9. Performance Specifications..... | 11 |
| 2.9.1. Simultaneous Users..... | 11 |
| 2.9.2. Capacity Limits..... | 11 |
| 2.9.3. Timing | 11 |
| 2.9.4. Transactions Process | 12 |
| 2.10. Quality Attributes Specification..... | 12 |
| 2.10.1. Software Quality Assurance (SQA)..... | 12 |
| 2.10.2. Coding Standards | 13 |
| 2.10.3. Error Handling Guidelines | 13 |
| 2.11. Reliability Specifications..... | 13 |
| 2.12. Scope Integration..... | 13 |
| 2.13. Security Specifications | 14 |
| 2.14. System Features | 14 |
| 2.15. Usability Specifications..... | 14 |
| 3. Applicable Standards | 15 |
| 4. Message Archive Capability..... | 15 |
| 5. Interfaces | 15 |
| 5.1. Communications Interfaces | 15 |
| 5.2. Hardware Interfaces..... | 15 |
| 5.3. Software Interfaces..... | 16 |
| 5.4. User Interfaces | 16 |
| 6. Legal, Copyright, and Other Notices | 16 |
| 7. Purchased Components..... | 16 |

| | |
|------------------------------------|----|
| 7.1. Defect Source (TOP 5) | 16 |
| 8. User Class Characteristics..... | 16 |
| 9. Estimation..... | 17 |
| 10. Approval Signatures | 18 |

1. Introduction

The Direct Project is an open-government initiative sponsored by the Office of the National Coordinator for Health Information Technology (ONC) under the Department of Health and Human Services (HHS), which has developed a specification for a simple, secure, scalable and standards-based method to send encrypted, health information directly to known, trusted recipients over the Internet. The Final Rule for Meaningful Use Stage 2, released in September 2012, requires use of Direct protocol to qualify for federal Electronic Health Record (EHR) certification; and 48 State Health Information Exchanges (HIEs) have planned support for the Direct Project as part of the federal State HIE Grant Program. These two factors make the Direct Project a major focus of the national HIE strategy and could lead to ubiquitous use among non-Veteran's Affairs (VA) Providers in the near future.¹

The Virtual Lifetime Electronic Record (VLER) Health Direct Development project (herein referred to as the Direct Secure Messaging Enhancements) provides the ability for VA Providers to exchange health information with external partners using the Direct standard. The Direct Secure Messaging Enhancements solution is a Government off the Shelf (GOTS) product, originally developed for DoD that is being customized and expanded for use by VA.

The Webmail Application provides the ability for the electronic exchange of information required to support fee basis authorization (including any additional health information relevant to the request) from VA to non-VA care providers. The Webmail Application also allows non-VA providers to return Direct messages back to the VA provider. This has the potential to enhance the timely delivery of care and improving health of Veterans and other beneficiaries. Direct Secure Messaging Enhancements also provides an Application Programming Interface (API) that allows VA enterprise systems to leverage the existing Direct capability, referred to as Direct as a Service (DaaS). DaaS is designed to be leveraged across multiple use cases, systems and applications for sending health information. Direct Secure Messaging Enhancements allows application and system administrators to manage access to the API through the API Admin Panel.

1.1. Purpose

This Requirement Specification Document (RSD) captures the requirements for establishing the scope and behavior of Direct Secure Messaging Enhancements. The Direct Secure Messaging Enhancements Development team has analyzed the business and functional requirements and the integration of new components into the existing system and its impact. Any supporting requirement documentation will be referenced, as needed. This RSD is a living document and contains the requirements captured and authored by the customer/business owner identified in the DSME Business Requirements Document (BRD). Any updates to requirements will be coordinated with the business stakeholder community, approved by the DSME Project Manager (PM), and any appropriate stakeholders.

¹ The Medicare and Medicaid EHR Incentive Programs provide a financial incentive (\$44,000) for the "meaningful use" of certified EHR technology to achieve health and efficiency goals.
https://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp

As work on the DSME project progresses and evolves, this document will continue to be updated so as to reflect the most current understanding. The RSD will be aligned to reflect the Business Requirements Document (BRD), Requirements Elaboration Document (RED), Requirements Traceability Matrix (RTM), and the System Design Documentation (SDD).

This document will capture the results of the requirement gathering phase of the System Engineering lifecycle, as described in the DSME Contractor Project Management Plan (CPMP) and Project Work Statement (PWS). The target audiences for this document are the DSME Development Team members, the functional community, stakeholders, system analyst and developers.

1.2. Scope

The purpose of Direct Secure Messaging (DSM) is to support electronic exchange of information over the Internet, using the Direct Project standards, published by the U.S. Department of Health and Human Services (HHS), the Office of the National Coordinator for Health Information Technology (HIT).

Direct Secure Messaging Enhancements consist of critical components of the Veterans Lifetime Electronic Record (VLER) framework to share healthcare information between federal agencies and non-federal entities thereby supporting quality and efficient healthcare for Veterans and active Service Members. The Direct Secure Messaging Enhancements Project is developing additional functionality that provides the secure exchange of medical record information between the VA, DOD, and private sector partners. Enhancements will improve the user experience and streamline system performance by addressing requirements which have changed, removed, or added from the 2010 NwHIN Direct BRD, the 2012 VA Direct BRD, and the VA Direct Secure Messaging RED.

This document outlines the requirements for the different areas of DSME.

Currently, the plan is to complete work in four increments. Associated requirements for specific increments are identified below under functional requirements.

Increment 1: Secure Messaging Functionality (8/15/15 - 2/14/16)

Increment 2: Secure Messaging Reports and Expanded Management Services (11/15/15 - 5/14/16)

Increment 3: Secure Messaging System Access (2/15/16 – 8/14/16)

Increment 4: Secure Messaging Electronic Receipt and Administrative Activities (5/15/16 – 11/14/16)

Specific requirements are captured within user stories and traceability in the RTM which contains all the business requirements to a level of detail as defined by ProPath sufficient to enable system design to satisfy requirements, and testers to test that the system satisfies those requirements. Within the RTM, every stated requirement will be externally perceivable by user story/case actors (i.e. users, stakeholders, or business owners). The requirements include a description of inputs (i.e. stimuli – requirements), outputs (i.e. responses - deliverables), and system functions in response to inputs or in support of outputs

1.3. References

The following documents should be referenced when reviewing the RSD:

- DSME Performance Work Statement (PWS)
- DSME Contractor Project Management Plan (CPMP)
- DSME Software Design Description (SDD)
- DSME Business Requirements Document (BRD)
- DSME Requirements Elaboration Document (RED)
- DSME Requirements Traceability Matrix (RTM)
- DSME Interface Control Document (ICD)
- DSME Production Operations Manual (POM)
- DSME Product Architecture Document (PAD)
- DSME Transition Plan
- TAC-13-06765 Direct Development Project Work Statement
- Applicability Statement for Secure Health Transport, versions 1.4 and 1.5

These documents can be found on the VA SharePoint Repository at the following link: [DSME Project Artifacts](#)

2. Overall Description

The DSME requirements within this document are described to a level of detail sufficient to enable the DSME Development Team to design a system that meets these requirements and to allow the DSME test team to create test acceptance criteria. Any further details or information needed will be posed to the functional stakeholders and DSME Project Manager (PM) for further clarification.

The Requirements Traceability Matrix (RTM) can be further reviewed for details on the traceability of each business requirement, to the subsystem (if applicable), use case and user story, to the system requirement, and test case scripts. The requirements documented within this document are aligned to the RTM for consistency.

2.1. Accessibility Specifications

The DSME system will be in 508 Compliance for user accessibility. Compliance with Section 508 will be determined by fully meeting the applicable requirements as set forth in the Veterans Health Administration (VHA) Section 508 checklists (1194.21, 1194.22, 1194.24, 1194.31 and 1194.41).

2.2. Business Rules Specification

This section outlines the applicable VA business rules that defines or constrains some aspect of the business process associated with the DSME system. Business rules can apply to people, processes, corporate behavior and computing systems in an organization.

For the DSME system, the system is designed to not focus solely on one business process or use case but instead for general use for secure Direct messaging exchange that can be applied to various use cases, leveraged by various enterprise systems and business processes.

2.3. Design Constraints Specification

This section outlines any design constraints on the DSME system being developed. This includes software languages, software development process requirements, prescribed use of development tools, architectural design constraints, purchased components, and class libraries.

The DSME system must adhere to Information Technology (IT) regulations for VA software development. Every release of DSME software testing shall undergo government testing and meet functional specifications and functional acceptance criteria. Through an agile development methodology, the DSME Development Team will continually incorporate functional user feedback. Table 1 lists some design constraint specifications from the PWS.

Table 1: Design Constraint Specifications

| Req ID | Requirement Description |
|--------|---|
| N/A | The system development shall follow the VA approved Software Development Life Cycle (SDLC), called out by PMAS and ProPath. |
| N/A | The system development shall apply software development processes of, or equivalent to, the Institute of Electrical and Electronics Engineers (IEEE) Standards, or the Software Engineering Institute (SEI) Capability Maturity Model (CMMI). |

2.4. Disaster Recovery Specification

The DSME system is located in the Austin Information Technology Center (AITC) and will rely on the disaster recovery and operations maintenance plans in place to support systems that require continuous availability. Information on Disaster Recovery Specification and Operational Maintenance is documented in the DSME Production Operations Manual (POM) and the Service-Level Agreement (SLA) with the AITC.

2.5. Documentation Specifications

The DSME Development team will ensure that all documentation developed is in compliance with VA documentation PMAS templates and specifications. The documentation to be delivered with each software release is detailed in the Development Contractor Project Management Plan (CPMP).

2.6. Functional Specifications

This section details the functional specifications for the DSME software for version 1.5.1. Any additional specifications for later software versions or releases will be incorporated into future versions of this document. The functional specifications within this section are organized according to Business Need (BN) from the DSME Business Requirements Document (BRD) and DSME Requirements Elaboration Document (RED).

BN 2: Provide basic secure messaging functionality that can be utilized without interruptions or deviations from regular workflows similar to products in use within VA today.

| OWNR Number | Owner Requirement (OWNR) | Comments | Priority* | Increment |
|-------------|---|---|-----------|-------------|
| 2.10 | Provide the ability for a Direct Secure Messaging System User to determine message delivery status, including Dispatched MDN. | According to current ONC Standards and Guidelines (version 2.0) | Medium | Increment 1 |

| OWNR Number | Owner Requirement (OWNR) | Comments | Priority* | Increment |
|-------------|---|--|-----------|-------------|
| 2.15 | Provide the ability for a Direct Secure Messaging System User to interact with inline end user context sensitive help for using the Direct Secure Messaging System, where the user does not have to leave their current location to access help in all cases. | Direct team is creating videos and we want the ability to have these linked from <u>within</u> the Direct system, as well as help in text form. | Medium | Increment 1 |
| 2.16 | Provide the ability for a Direct Secure Messaging System User to view understandable system error messages that inform the user of any errors encountered related to activities performed within the Direct Secure Messaging System. | Ongoing requirement. This is met to some degree in the current versions of Direct. | High | Increment 1 |
| 2.22 | Provide the ability for a Direct Secure Messaging System User to use the preview capability for files that can be attached or that are already attached to a Direct secure message before sending the message. | In Web Portal - Right now a pdf document opens in another window. Make this easier, e.g. Hover over and see the information about the document without opening the entire document or preview on the side. Patient safety issue. | Low | Increment 1 |
| 2.26 | Provide the ability to send a message to all VA Direct Users from within the Direct Secure Messaging System. | | High | Increment 1 |
| 2.27 | Provide the ability to send an automatic reply type message, e.g. "out of office" message, from within the Direct Secure Messaging System that could be transmitted both within and outside the VA Direct System for a personal mailbox (individual user). | This would apply to a personal mailbox only. | High | Increment 1 |

| OWNR Number | Owner Requirement (OWNR) | Comments | Priority* | Increment |
|--------------------|--|---|------------------|------------------|
| 2.28 New | System will have the ability to block a single organization in a HISP or end user within an otherwise trusted partner HISP. | VA Returns a message that VA has blocked the specific address and to please contact Direct Program Manager for more information | Low | Increment 1 |
| 2.29 New | Provide the ability to send a notification message to the VA Direct team's regular email address (Outlook) when a message is received in the Direct Feedback Log (mailbox) | Like the notification messages sent to the users regular email when a Direct message is received | High | Increment 1 |

BN 3: Provide basic secure messaging (email) functionality that allows administrative users to perform an array of administrative activities for managing users, groups and directories within the Direct Secure Messaging System.

| OWNR Number | Owner Requirement (OWNR) | Comments | Priority* | Increment |
|--------------------|--|---|------------------|------------------|
| 3.5 | Provide the ability for a VA Direct Secure Messaging System User (Web Portal and Direct as a Service) to discover and search the Healthcare Directory of a trusted non-VA partner organization Healthcare Directory. | If partner directory is not searchable, directory information will have to be exchanged out of band, e.g. phone or regular email communication. National standards are being developed. Should be an optional task for a contract in case the standard is not in place during the term of the contract. | Medium | Increment 4 |
| 3.6 | Provide the ability for a trusted non-VA Direct partner organization to discover and search the VA Internal Enterprise wide Direct Secure Messaging System Healthcare Directory. | National standards are being developed. Should be an optional task for a contract in case the standard is not in place during the term of the contract. | Medium | Increment 4 |

BN 4: Provide the ability to create/run /view/print reports utilizing role based traits with varying degrees of access/authority within the Direct system

Business Need 5: Provide expanded services to manage both inpatient and outpatient request for services.

| OWNR Number | Owner Requirement (OWNR) | Comments | Priority* | Increment |
|--------------------------|--|---|------------------|------------------|
| 5.3 Elaborated | Provide the ability to prevent the editing of received C-32 or C-CDA content in the Direct Secure Messaging System. | To ensure that the document received and uploaded in Veteran record is the same as that sent. | Medium | Increment 2 |
| 5.4 Elaborated | Provide the ability for the Direct Secure Messaging System to facilitate the action required to save received C-32 or C-CDA content within appropriate VA systems, e.g. CPRS or DAS. | Meaningful Use: May not be fully automated, but Direct needs to be compatible with process that exists today to incorporate data into the record without creating a new work process. Note: AVS folks have a way to do this. DAS?Policy? | Low | Increment 2 |
| 5.5 | Provide the ability to select items from received C-CDA content to be extracted into a separate file. | If VA Policy will permit this. We should wait until the HL7 recommendations about tagging each section of CCDA with author/contributor/electronic signatures is done before permitting the C-CDA to be treated as anything but the whole document | Low | Increment 2 |
| 5.6 | Provide the ability to save extracted item (s) of received C-CDA content (to include associate patient/provider identifiers) into a file separate from the C-CDA. | If VA Policy will permit this. We should wait until the HL7 recommendations about tagging each section of CCDA with author/contributor/electronic signatures is done before permitting the C-CDA to be treated as anything but the whole document | Low | Increment 2 |

| | | | | |
|--------------------------|--|---|--------|-------------|
| 5.7 New | Provide the ability for the Direct System to query the Veterans Authorization and Preference System (VAP) to determine that a Veteran has authorized sending his/her data when there is an automated sending of C-32 or C-CDA via Direct System. | The automated send would be triggered by an event such as an update to the record or the need to send VA CCDA or C32 to an HIO data base. | High | Increment 2 |
| 5.8 Elaborated | Provide the ability to send a C-CDA or C-32 document via the VA Direct Secure Messaging System to a partner Direct system. | We currently have ability to send as PDF. We are transitioning to CCDA with style sheet. We want this on both Web Portal and available to Direct as a Service | High | Increment 2 |
| 5.9 New | Provide the ability for the Direct System to display and incorporate a CCR received from a non-VA partner | This meets MU 2014 Certification | Medium | Increment 2 |
| 5.10 New | Provide the ability to preview an attached xml document, e.g. CCDA, using the VA style sheet | It could be a separate window or preview pane (preferred for patient safety feature to avoid multiple documents open to be viewed). | High | Increment 2 |

Business Need 6: Electronic receipt into the Direct Secure Messaging System of results of imaging services performed by non-VA care providers and transmission of VA images to non-VA providers via the Direct Secure Messaging System.

| OWNR Number | Owner Requirement (OWNR) | Comments | Priority* | Increment |
|-------------|---|---|-----------|-------------|
| 6.1 | Provide the ability to receive images shared by the non-VA care provider and store within VA systems as authorized. | Provide the ability to receive images shared by the non-VA care provider regarding the Veterans medical history. | Low | Increment 4 |
| 6.2 | Provide the ability to send images to a non-VA care provider. | Very large file or a link to a very large file (e.g. DICOM reports to an external non-VA recipient. Currently sizes are limited to 4MB. | Low | Increment 4 |

Business Need 7: Provide the ability to access the Direct Secure Messaging System when working in other interfacing applications without having to be logged into the Direct system.

| OWNR Number | Owner Requirement (OWNR) | Comments | Priority* | Increment |
|-------------|--|---|-----------|-------------|
| 7.1 | Provide the ability for a Direct Secure Messaging System User to manage Direct secure messages when working in other applications where the Direct Secure Messaging System can either be launched or accessed. | This should occur without having to be first logged into the Direct Secure Messaging System. Provider does not want to have to log in to another system to work outside normal workflow. CCOW compliant is an option. | Medium | Increment 3 |
| 7.2 NEW | Provide the ability for Direct to recognize patient context for a patient record selected in an application (for example, CPRS or eHMP) accessing Direct functionality. | | | Increment 3 |

| | | | | |
|-------------------|---|--|------|-------------|
| 7.3 NEW | Provide the ability for a third-party application to use a Direct widget to take advantage of the Direct As a Service. Widget would allow other software to include all Direct functionality, e.g. inbox, a compose message screen in their software user interface, access Healthcare Directories. | Direct provides a few lines of code that would be included by the other software package to create a “widget.” User Story: A user in the CPRS application selects the widget and a Direct compose screen opens, allowing the user to attach a document, e.g. progress note, to a Direct message and send it to the non-VA Direct recipient entered in the To: line. | High | Increment 3 |
|-------------------|---|--|------|-------------|

BN9: Provide access to test and demonstration environment(s) for Direct.

| OWNR Number | Owner Requirement (OWNR) | Comments | Priority* | Increment |
|--------------------|---|---|------------------|------------------|
| 9.3 | Provide the ability to access demonstration instance(s) of the Direct Secure Messaging System. | <u>Two</u> demonstration environments are needed to be created and maintained that mirror production and development increments environments. | High | Increment 1 |
| 9.4 New | Set up and maintain a logically separated Direct System production environment to use for Veteran Initiated use of the Direct System. | Would contain all certificates in provider to provider system (FBCA cross certified), as well as certificates accepted for patient only transmission. | High | Increment 1 |
| 9.5 New | Set up and maintain a Direct System environment in the VA Innovations “Sandbox.” | This would contain the latest production version of the Direct System software | Medium | Increment 1 |

2.7. User Interface (GUI) Specifications

The GUI for DSME was already developed in previous work – refer to Direct Secure Messaging Requirements Specification Document v1.5.

2.8. Multi-divisional Specifications

There are currently no requirements for the DSME system regarding multi-divisional specification at the time of this release.

2.9. Performance Specifications

The performance specification such as the number of simultaneous users, transactions, tasks, and date to be processed within certain time periods for both normal and peak workload conditions ensure that the DSME software is developed to meet functional stakeholder needs.

2.9.1. Simultaneous Users

The GOTS DoD Direct infrastructure was designed to handle at least 25 concurrent users performing transactions simultaneously. Under performance testing the application was shown to easily support that number.

The system will experience exponential growth as more VA partners implement Direct messaging. It is envisioned that the number of users will at least double annually for many years. Additional use will be driven by Direct's role in Meaningful Use Criteria.

2.9.2. Capacity Limits

This section details the capacity limits associated to the DSME system.

- The GOTS DoD Direct solution was designed to support 55,000 message transactions weekly, with a peak load of 330 messages per hour.
- In the initial stages, messages will be either text, or more likely, messages with a several page attachment. The DSME system currently has a 10 MB limit. Generally messages will be smaller than 1 MB.
- At the Mountain Home VAMC, there is an average of 59 mammograms ordered each month.
- In FY 2009, the number of screening mammograms performed across the enterprise via non-VA purchased care was 19,576; in FY 2010, there were 18,400 screening mammograms performed.

At the time of the release of this document, the capacity limit requirements for use of the API Admin Panel and the API have not been decided.

2.9.3. Timing

This section details the timing specifications associated to DSME as shown in Table 10.

Table 2: Timing Specifications

| Req ID | Requirement Description |
|--------|---|
| N/A | The system shall provide response times and page load times consistent with standards for similar applications. |
| N/A | The DSME system will respond to user actions in 3 seconds or less, 90% of the time, and never more than 10 seconds. |

2.9.4. Transactions Process

The following requirements pertaining to transaction processes have been gathered from the DSME BRD.

- Information about response time degradation resulting from unscheduled system outages and other events that degrade system functionality and/or performance will be disseminated to the user community within 30 minutes of the occurrence. The notification will include the information described in the current Automated Notification Reporting (ANR) template maintained by the VA Service Desk. The business impact must be noted.
- With system downtime taken into consideration, DSME users will be able to utilize a basic secure messaging system that does not present constraints on their ability to process through workflows at least 95% of the time.
- The DSME Secure Messaging System will be available 99.5% of the time. Even during system outages, all messages will be handled properly—either resending messages automatically once the system is available or clearly alerting the sender that the transmission failed. This 99.5 percentage is different from the 99.9% availability percentage requirement reported in the BRD and RED. This document will supersede the availability percentages reported in the BRD and RSD in order to comply with the SLA with the AITC. This 99.5% availability change was agreed to by the Business Sponsor in an email dated March 20, 2015 and can be found on the project SharePoint site.
- 100% of the DSME Secure Messaging System Accounting of Disclosures will be recorded and accessible to appropriate users in the VAP system.
- All administration (e.g. maintaining user DSME addresses, setting up groups, maintaining distribution lists, etc.) is done 90% of time without specific support from the national development team.
- Notification of scheduled maintenance periods that require the service to be offline or that may degrade system performance will be disseminated to the DSME System user community a minimum of 48 hours prior to the scheduled event.

2.10. Quality Attributes Specification

This section details the specifications that enhance the supportability, maintainability, portability, testability, or reusability of the DSME system being developed. The DSME system will adhere to industry best practices and standards.

2.10.1. Software Quality Assurance (SQA)

The DSME Development team will implement software quality procedures that will ensure delivery of high quality code free of critical bugs or vulnerabilities. The DSME Development Team will:

- Develop a Master and Release Test Plan that outlines the execution of Test Scenarios and Test Procedures mapped to the Business Requirements Document.
- Implement automated test scripts built for efficient regression, messaging, performance, and capacity testing.

- Conduct Software Code Quality Checking (SCQC) throughout development and testing through the use of static and dynamic code scans.
- Use Fortify to ensure the development of code that introduces 0 high and 0 critical vulnerabilities.
- Support Independent Verification and Validation (IV&V) and User Acceptance Test (UAT) efforts
- Ensure all code changes are tracked through change requests submitted, monitored and implemented through Rational Jazz.
- Quality Assurance Surveillance Plan (QASP) will be submitted throughout the life of the project to ensure that the DSME Development Team provides acceptable service and deliverables.

2.10.2. Coding Standards

The DSME Development Team adheres to a set of Coding Standards based on industry best practices that are given to all members of the development team and are subject to annual review and update. Review and update will also take place when any of the following situations occurs:

- Changes in scope or management processes that necessitate a change in coding standards
- Identification of process improvement activities
- Changes in tools and techniques

2.10.3. Error Handling Guidelines

The DSME Development Team conforms to the PEAR PHP guidelines for error handling per <http://pear.php.net/manual/en/standards.errors.php>.

2.11. Reliability Specifications

The system needs to be available on a 24-hour a day basis, 7 days a week. While the administrative staff will be working business hours, non-VA providers may wish to return results to the VA at alternative times of the day. The system needs to be available to accept results at any time. The following reliability requirements, Table 11, were obtained from the BRD.

Table 3: Reliability Specifications

| Req ID | Requirement Description |
|--------|--|
| N/A | <p>The system shall be reliable and enable user trust, by providing the following:</p> <ul style="list-style-type: none"> • Stable and reliable performance; • Accurate data; • Display of all data that is available in native or interfaced systems and intended to be available in the application; and • Accessible information related to the source of data. |

2.12. Scope Integration

This section details the integration of the DSME system to other products. For increments 1 and 2 there will be no new integration with other systems.

2.13. Security Specifications

This section details the security specifications for the DSME system as shown in Table 12.

Table 4: Security Specifications

| Req ID | Requirement Description |
|--------|--|
| N/A, | The system shall allow users to login to the DSME system using a VA issued PIV ID. |
| ENTR25 | All VA security requirements will be adhered to. Based on Federal Information Processing Standard (FIPS) 199 and National Institute of Standards and Technology (NIST) SP 800-60, recommended Security Categorization is High. The Security Categorization will drive the initial set of minimal security controls required for the information system. Minimum security control requirements are addressed in NIST SP 800-53 and VA Handbook 6500, Appendix D. |

2.14. System Features

Table 13 provides an overview of the different components of the DSME system and the inputs and outputs of each component.

Table 5: Overview of System Features

| System Feature | Inputs | Outputs | Threshold Product | Objective Product |
|----------------------------------|--|--|-------------------|-------------------|
| Secure Messaging Web Portal | Message Content, Direct Address (into main Webmail Client) | Standard Direct Message, delivered to intended recipient | Required | Required |
| Secure Messaging Admin Panel | User/Group Information | Usage Statistics, Approved/Rejected Users | Required | Required |
| Secure Messaging API | Message Content, Direct Address (through Web Services) | Standard Direct Message, delivered to intended recipient | Required | Required |
| Secure Messaging API Admin Panel | System Information | Usage Statistics, API Keys | Required | Required |

2.15. Usability Specifications

TBD

3. Applicable Standards

DSME must comply with current ONC Standards and Guidelines (version 2.0) for implementing the Applicability Statement for Secure Health Transport as shown in Table 15.

Table 6: Implementation Requirements

| Req ID | Requirement Description |
|---------------------------|---|
| Option-NONF2759-PWS 5.6.3 | End user functionality and training documentation and materials for the Direct application shall be provided in conjunction with the installation of incremental software releases in the SQA Environments (every six months or earlier). |
| Option-NONF2762-PWS 5.6.3 | Email functionality shall be developed in accordance with ONC and similar governing bodies standards for Direct. |
| Option-NONF35-PWS 5.6.4 | Demographic information will be exchanged using Health Information Technology Standards Panel (HITSP) standard terminologies. |

4. Message Archive Capability

The DSME system's patient consent directives and a full accounting of patient information disclosures will be archived and stored for 75 years as shown in Table 16.

Table 7: Data Back-up/Archive Requirements

| Req ID | Requirement Description |
|----------------------------|--|
| Option-NONF21-PWS 5.6.12 | Provide the ability to retain the accounting of disclosures for up to 75 years, as required by Privacy Act as the life of the EHR is 75 years. |
| Option-NONF2776-PWS 5.6.12 | Provide the ability to retain consent directives for up to 75 years. |

5. Interfaces

This section is intended to define the interfaces the application will support and include adequate specificity, protocols, ports, and logical addresses so that the software can be developed and verified against the interface requirements. User, hardware, software, and communications interfaces should be included in this section.

5.1. Communications Interfaces

This section describes any communication interfaces to other systems or the interfaces within the AITC environment. The reference technical architecture descriptions, as developed by DSME system architects (SAs), can be found in the SDD and Product Architecture Document (PAD).

5.2. Hardware Interfaces

This section defines any hardware interfaces that support the DSME system, including logical structure, physical addresses, etc. For the DSME software, reference technical architecture descriptions can be found in the SDD and PAD.

5.3. Software Interfaces

This section is meant to detail the software interfaces to the DSME system. These include purchased components, components reused from another application, or components being developed for subsystems outside of the scope of this project. For DSME, all interfaces are documented in the SDD and the PAD.

5.4. User Interfaces

The DSME system will have a user interface that has been created specifically for VA use of Direct software functionality, referred to as the DSME Webmail application. The webmail application is described in the SDD. Additionally, there is a user interface for application administrators to manage their' applications access and use of the VLER Direct API web services, referred to as the API Admin Panel. This is further detailed in the SDD.

6. Legal, Copyright, and Other Notices

Section not applicable.

7. Purchased Components

Section not applicable.

7.1. Defect Source (TOP 5)

Section not applicable.

8. User Class Characteristics

The User Class Characteristics, Table 17, were obtained from the DSME BRD.

Table 8: User Characteristics

| User Characteristics | | |
|----------------------|--|---|
| Primary Users | VA care provider | <ul style="list-style-type: none">• Create consults• Receive consult results• Inform patients of results• Create orders and notes in CPRS. |
| | Non-VA healthcare providers and administrative staff | <ul style="list-style-type: none">• Receive consults and additional information from VA providers• Schedule and perform mammograms• Create reports and send to VA• Phone/page VA providers when results are abnormal |
| | VA Administrative Staff in NVCC (Fee Basis) Office | <ul style="list-style-type: none">• Perform case management• Obtain authorization for cares |

| User Characteristics | | |
|----------------------|--|---|
| | | <ul style="list-style-type: none"> • Schedule appointments/provide appointment information to patients • Send authorization for cares and additional information to non-VA care providers • Receive, scan, store and index results |
| | VA Release of Information (ROI) Office Staff | <ul style="list-style-type: none"> • Ensures each request for patient data and health care information has a valid authorization prior to disclosure • Coordinates disclosures of protected health information • Maintain an accounting of disclosures |
| Secondary Users | Local VA IT staff | <ul style="list-style-type: none"> • May need to assist with certain aspects of testing and implementation |
| | Privacy Staff | <ul style="list-style-type: none"> • Ensure Veteran information is appropriately protected when sending information between VA and non-VA care providers |
| | Health Information Management (HIM) Staff | <ul style="list-style-type: none"> • Manage health information and patient health records • Advise on business processes related to releasing Veteran PHI • May be involved in activities related to scanning results received via the Direct System into the VA medical record • Use the system to generate reports and monitor program implementation |
| | Health Information Management (HIM) Staff | <ul style="list-style-type: none"> • Manage health information and patient health records • Advise on business processes related to releasing Veteran PHI • May be involved in activities related to scanning results received via the Direct System into the VA medical record • Use the system to generate reports and monitor program implementation |

9. Estimation

This section will be updated when the functional point analysis is completed.

