*VistA Laboratory Enhancements (VLE) Project: Autoverification Initiative*

**VistA Auto Release Capability**

**Requirements Specification Document**



**Department of Veterans Affairs**

**October 2015**

**Version 0.05**

**Revision History**

Note: The revision history cycle begins once changes or enhancements are requested after the

Requirements Specification Document has been baselined.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 10/21/2015 | .05 | Functional and Non Functional  Requirements from RRC |  |
| 05/26/2015 | .04 | Updated Function Point Count |  |
| 5/13/2015 | .03 | Peer Review |  |
| 5/12/15 | .02 |  |  |
| 4/24/2015 | .01 | Initial draft |  |

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **1.** | **In** | **troduction ........................................................................................ 4** |
|  | **1.1.** | **Purpose ............................................................................................................ 4** |
|  | **1.2.** | **Background ...................................................................................................... 4** |
|  | **1.3.** | **Scope ................................................................................................................ 5** |
|  | **1.4.** | **Assumptions .................................................................................................... 6** |
|  | **1.5.** | **References ....................................................................................................... 6** |

**2. Overall Description ............................................................................ 6**

**2.1. Accessibility Specifications............................................................................ 6**

**2.2. Business Rules Specification ......................................................................... 6**

**2.3. Design Constraints Specification................................................................... 6**

**2.4. Disaster Recovery Specification .................................................................... 6**

**2.5. Documentation Specifications........................................................................ 6**

**2.6. Functional Specifications ............................................................................... 7**

**2.7. Non Functional Specifications........................................................................ 9**

**2.8. Features .......................................................................................................... 16**

**3. Applicable Standards ...................................................................... 17**

**4. Interfaces .......................................................................................... 17**

**4.1. Communications Interfaces .......................................................................... 17**

**4.2. Hardware Interfaces....................................................................................... 17**

**4.3. Software Interfaces........................................................................................ 17**

**4.4. User Interfaces ............................................................................................... 17**

**5. Legal, Copyright, and Other Notices .............................................. 17**

**6. Purchased Components .................................................................. 17**

**6.1. Defect Source (TOP 5) ................................................................................... 17**

**7. User Class Characteristics.............................................................. 17**

**8. Estimation ........................................................................................ 18**

**9. Approval Signatures ........................................................................ 20**

**1. Introduction**

The Vista Evolution Laboratory Enhancement of AutoVerification incorporates Decision Support Algorithms or rule sets to automatically review laboratory results and directly post “normal” results to the patient’s chart. Results that are deemed “abnormal” by the rule set will be reviewed by laboratory personnel before being manually released into the patients electronic health record (EHR). AutoVerification will address staffing deficiencies, increase patient safety, decrease manual workload, decrease result turnaround times and reduce costs by automating the result review and charting process.

**1.1. Purpose**

The purpose of this Requirements Specification Document (RSD) is to convey the analysis and requirements associated to the delivery of enhancements to the Veterans Health Information Systems and Technology Architecture (VistA) Laboratory AutoVerification, VistA Auto Release Capabilities. This is a subset of capabilities of the full

Autoverification initiative and focus on the changes needed to VistA Legacy Laboratory System.

Currently, all laboratory test results, both normal and abnormal, are required to be manually reviewed and approved by lab technologists before release.

Since the vast majority of lab test results fall in the “normal” range, this translates into a

much larger workload for the technologists. By automating verification of normal test results, technologists will have more time to devote to analysis of abnormal test results. The Laboratory AutoVerification process involves automatic review of test results on a lab-established set of boundaries, also referred to throughout this document as rules, rule sets and decision support algorithms. This process will eliminate the need for a qualified technologist to manually approve all “normal” results before they are sent to the patients’ electronic health record (EHR) for clinicians to view.

The intended audience for the RSD includes, but is not limited to, the VistA Lab Working Group members that includes; Project Managers, Analysts, Developers, Testers, Technical writers, and the Business users and consumers of the data.

**1.2. Background**

Veterans Health Administration (VHA) sponsored an Employee Innovation Challenge in

2013. VA employees were invited to identify the most important challenges that, if solved, would meaningfully increase quality, improve access, increase Veteran

satisfaction, and lower costs of meeting the needs of Veterans, their dependents, and caregivers. The Laboratory Auto-Verification presentation was carefully reviewed and

chosen due to its compelling potential to improve the accessibility, quality and overall effectiveness of VA as it seeks to deliver the highest quality services to our nation's Veterans.

A pilot solution was developed specifically for the Kansas City Veterans Affairs Medical Center (KC VAMC). KC VAMC configured the Instrument Manager System to introduce Decision Support Algorithms or rule sets to provide auto-verification within its Clinical Chemistry department. The Instrument Manager System is licensed to VAMC under a separate license agreement. The Pilot included the design and implementation of chemistry rule sets and introduced these rule sets into the production Data Innovations

Instrument Manager system currently in use at KC VAMC. Consultation was also acquired for BioRad Unity Real-Time Quality Control (QC) Integration, Moving Averages, eCAP Solutions, and Lab Intelligence Reports Manager software logic for three environments (Production, Shadow and Test).

This model of autoverification uses a middleware system that passes lab results,

coming from the lab instruments, through a rule set that determines if the results fall in a

“normal” or “abnormal” range. If the lab result passes the rule set, it is given a special character in the Observation Request (OBR) segment that is inserted in an HL7 message and sent directly to the VistA Lab global. If a lab result cannot pass the rule set, it is held in the middleware system for review by a lab technologist. Once the technologist deems the result appropriate for release, it is released from the middleware system and goes to VistA Lab global with the special character in the OBR segment of an HL7 message. The Kansas City Class III MUMPS code recognizes this special character and automatically processes these results out of the global for availability in VistA and the Computerized Patient Record System (CPRS).

Lab instruments can be set up as either available for autoverification or not available for autoverification. Those that are available for autoverification will have the review process done in the middleware. Those instruments not available for autoverification

will have the lab results pass from the lab instrument through the lab middleware to the

Vista global. The lab technologist must review each lab result using current Vista menus (EA and EM)

**1.3. Scope**

The scope for this VistA Laboratory Auto Release enhancement includes:

• Receiving an indication of when a test has been successfully autoverified within the middleware (DI).

• Processing test results, with an indicator of successful autoverification, to Auto Release, making results available to appropriate clinicians and providers with privileges to view the results.

• Receiving an indication of when a test has been successfully verified by an authorized technologist.

o This is only for Tests that fail the autoverify rule on DI, and tech with a VistA DUZ/record will manually verify on DI and then the result will include the techs id with the results.

 Any results performed on a designated Autoverification instrument will be verified by rules set on DI or manually by a lab technician.

 Delta checks, critical values, instrument flags, specimen specific conditions, etc. functionality currently within VistA will be maintained, even with Autoverified results.

 DI will always have only a subset of result data available.

 Reference Ranges will be maintained both in VistA and in the DI

middleware.

• Processing test results, with an indicator of successful verification by an authorized technologist, to Auto Release, making results available to appropriate clinicians and providers with privileges to view the results.

• Sending ordering provider contact information to the instrument middleware for the purpose of making it accessible to authorized technologists who are responsible for verifying test results, contacting caregivers.

**1.4. Assumptions**

There will be no changes to Corrected Results, handled in VistA lab as per SOP.

**1.5. References**

• VistA Evolution Program Charter

• VA Handbook 6500 – Information Security Program

• VLE Laboratory Autoverification Enhancements Requirements Specification Document 2

March 2015

• Vista Evolution Program Plan

• VE Lab AutoVerification Business Requirements Document (BRD) and Requirements Traceability Matrix (RTM:

• VistA Laboratory Packages:

• CPRS GUI:

• CPRS Technical Manual:

• Dawning Instrument Guide:

• Data Innovations Instrument Gui

**2. Overall Description**

**2.1. Accessibility Specifications**

The product will comply with 508 specifications.

**2.2. Business Rules Specification**

The BRD lists all business requirements for this enhancement.

**2.3. Design Constraints Specification**

Design constraints will be documented in the System Design Document

(SDD).

**2.4. Disaster Recovery Specification**

The Laboratory module is part of VistA and will be covered under the current

VistA Disaster Recovery Plan.

**2.5. Documentation Specifications**

• Applicable guides and manuals, required to comply with the VA and Product Development (PD) documentation standards and/or ProPath requirements, will be provided.

• Updates will be made, as necessary, to applicable user manuals and other training tools and will be delivered to all levels of users. If no user documentation exists, it will be produced.

• A Requirements Traceability Matrix (RTM) will track requirements traceability.

• An implementation plan will be developed for the national deployment of Lab

AutoVerification and one for the VistA Auto Release Capability.

• Training documentation associated with the training curriculum (if deemed necessary) must be developed for Lab AutoVerification. We will update applicable user guides for the VistA Auto Release Capability.

• This Requirements Specification Document (RSD) documents the functional and non- functional requirements.

• The System Design Document (SDD) will document the design constraints related to functional requirements.

**2.6. Functional Specifications**

ID Contents

**User Story: Receive an indicator as AutoVerified**

566498

566499

566500

566501

• As a technologist, I want to know which results in VistA have been verified by the autoverification system, so that I can ensure compliance with all accreditation standards and best practices.

**Acceptance Criteria: Receive an indicator as AutoVerified**

• Results received from autoverification system contain an indication that the result is ‘AutoVerified’.

• VistA stores the indicator received from the autoverification system with the result.

• VistA stores the original message transmission for a period of time, as per current VistA capabilities, for troubleshooting purposes.

**User Story: Automatically Release AutoVerified Results**

• As a technologist, I want autoverified results sent to VistA laboratory system to automatically release, so that clinicians treating the patients can have immediate access to the result.

**Acceptance Criteria: Automatically Release AutoVerified Results**

• Results received from autoverification system that are identified as

‘AutoVerified’ will be automatically released and visible to the clinicians authorized to view the results (as per current VistA/CPRS capabilities) for the patient.

• Clinicians with appropriate authorization will immediately be able to view the patient’s autoverified results via CPRS.

566502

566503

566504

566505

566506

566507

566508

**User Story: Display identification of technologist who verified the result**

• As a technologist, I want to know which results in VistA have been verified by a technologist on the autoverification system, so that I can ensure it is

included with the results as well as compliance with all accreditation standards and best practices.

**Acceptance Criteria: Display identification of technologist who verified the result**

• Results received from autoverification system contain unique identification of the technologist who ‘Verified’ the result.

• VistA stores the identification of the technologist received from the autoverification system with the result.

• VistA stores the original message transmission for a period of time, as per current VistA capabilities, for troubleshooting purposes.

**User Story: Receive an indicator as Verified by Technologist.**

• As a technologist, I want verified results sent to VistA laboratory system to automatically release, so that clinicians treating the patients can have immediate access to the result.

**Acceptance Criteria: Receive an indicator as Verified by Technologist.**

• Results received from autoverification system, that are identified as ‘Verified’ will be automatically released and visible to the clinicians authorized to view the results (as per current VistA/CPRS capabilities) for the patient.

• Clinicians with appropriate authorization will immediately be able to view the patient’s verified results via CPRS.

• Ability to identify if the results were verified automatically or verified by lab technician, and will include unique VistA tech identifying code or name

**User Story: Look up Ordering Provider Information**

• As a technologist, I want to be able to look up ordering provider contact information during the verification process, so that I can easily obtain the information while verifying a result and not have to log on to another system.

**Acceptance Criteria: Look up Ordering Provider Information**

• VistA Laboratory system will include the provider’s pager and phone number available from New Person File #200, prior to the technologist initiating the results verification process.

• VistA stores the original message transmission for a period of time, as per current VistA capabilities, for troubleshooting purposes.

**User Story: Notify Users if Autoverification system fails to post results to VistA.**

• As a Medical Technologists, I want to be notified if a result is received from the Autoverification system by VistA and does not successfully save to the database, so that I can intervene to ensure the results are appropriately and promptly reported to clinicians.

566509

566510

566511

566512

566513

**Acceptance Criteria: Notify Users if Autoverification system fails to post results to VistA.**

• When a result fails to be processed on VistA, the system will log a Lab Universal Interface (UI) error/exception and generate an alert to designated users.

• When a result fails to be processed on VistA, a notification to DI – via an HL7 acknowledgment message with exception/error observed similar to status sent to POC COTS system after processing POC results.

**User Story: Save and store autoverified results with an indicator**

• As a technologist, I want to be able to look up results on the VistA and CPRS systems and determine whether or not it was autoverified, so that I can be assured the method of results verification and follow up if needed to ensure quality of results produced.

**Acceptance Criteria: Save and store autoverified results with an indicator**

• Patient result reports indicate results that are autoverified.

**User Story: New Auto Release capability tested in test environment prior to implementing in production.**

• As a technologist, I want to be able to test the new autoverification system with my VistA test system, so that I can adequately test the autoverification rules and system processing prior to implementing in a production environment.

**Acceptance Criteria: New Auto Release capability tested in test environment prior to implementing in production.**

• VistA Patch successfully installs into VistA Test Systems.

• VistA Field Test site’s Laboratory System can be connected to a local autoverification system prior to production release and used for testing autoverification rules, results posting, and auto release of results to CPRS.

**2.7. Non Functional Specifications**

|  |  |
| --- | --- |
| ID | Contents |
| 620304 | **Multi-divisional Specifications -** The VistA Auto Release Capabilities, must be  able to work with VistA Laboratory Systems operational in multi-divisional environments. |
| 620305 | **Performance Specifications -** Performance requirements can be found in the  “Performance, Capacity, and Availability Requirements” section in the Business Requirements Document (BRD). |

620306

620307

620308

**System Performance Reporting Requirements -** Include instrumentation to measure all performance metrics specified in the Non-Functional Requirements section of the Requirements Traceability Matrix (RMT). At a minimum, systems will have the ability to measure reporting requirements for Responsiveness, Capacity, and Availability as defined in the non-functional requirements section of the RTM. **System Performance Reporting Requirements** - Make the performance measurements available to the Information Technology (IT) Performance Dashboard to enable display of “actual” system metrics to customers and IT staff. **Quality Attributes Specification -** In accordance with the Office of the National Coordinator for Health Information Technology’s Meaningful Use Stage 2 final ruling, employ and industry recognized User Centered Design (UCD) process. The methods for UCD are well defined in documents and requirements such as ISO

9241-11, ISO 13407, ISO 16982, National Institute of Standards and Technology

Interagency Report 7741, ISO/International Electrochemical Commission 62366 and ISO 9241-210. Developers will choose their UCD approach; one or more specific UCD process will not be prescribed.

620309 **Reliability Specifications** - Consistent with VistA uptime at 99.9%.

**Scope Integration** - Lab AutoVerification module must be interoperable with other

620310

620311

620312

620313

620314

software systems including: VistA Laboratory (Lab) The VistA Lab service is one of the core VistA Lab packages that processes, stores and transmits Lab Order data and results.

**Scope Integration** - Laboratory System Re-Engineering Project (LSRP)

The LSRP system is a Laboratory Information Management System (LIMS) for the VA Pathology and Laboratory Medicine Service (PLMS). It was developed as a replacement for the current VistA Lab system but was only deployed at one site - the Huntington VAMC. The system uses Cerner Millennium PathNet, a Commercial Off-The-Shelf (COTS) LIMS. The Cerner Millennium PathNet is interfaced with

VistA to maintain system integration with the more than 40 applications currently receiving and/or providing information from VistA.

**Scope Integration** - Laboratory Middleware System (Data Innovations)

The Laboratory Middleware system supports the preparation of laboratory data, process and communication between VistA and the instrument for Lab AutoVerification. It also translates laboratory information and results from the instrument and shares it with Most VHA Labs use Instrument Manager as the middleware. It is estimated that only 7 VHA Labs use Dawning middleware. Both Instrument Manager and Dawning are owned by Data Innovations. It is assumed that sites using Dawning will have the option to convert to Instrument Manager as the middleware.

**Security Specifications** - VistA Laboratory Enhancements shall comply with all VHA Security, Privacy and Identity Management requirements including VA Handbook 6500.

**Security** - All VA security requirements will be adhered to. Based on Federal Information Processing Standard 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.

620315 **VE: Security and Privacy** All VA security requirements as defined in VA Handbook

6500 shall be followed. To assist BRD development, the Security Requirements

620316

620317

620318

Steering Committee (SRSC) has made available an authoritative extract of those requirements.

**VE: Security and Privacy** - All NIST SP 800-53 security control family requirements shall be followed. An extract of VA cross-cutting enterprise security and privacy requirements (categorized by current NIST SP 800-53 security control families) is available from the VA SRSC.

**VE: Security and Privacy** - Relevant Health Insurance Portability and Accountability Act (HIPAA) security and privacy requirements shall be followed. An extract of HIPAA requirements is available from the VA SRSC. An extract of HIPAA security requirements to be implemented in health care-related projects is available from VHA Health Care Security Requirements.

**VE: Security and Privacy** - Provide data sensitivity and segmentation support for

HL7 Version 3 Standard: Privacy, Access and Security Service; Release 1, Section

6.1.1, table 5: Data Segmentation Business Requirements.

620319 **Operational Environment Requirements -** System response times and page load times shall be the same or better than the current VistA system.

**Operational Environment Requirements -** Maintenance, including maintenance of externally developed software incorporated into the application(s), shall be

620320

620321

scheduled during off peak hours or in conjunction with relevant maintenance schedules. The business owner should provide specific requirements for establishing system maintenance windows when planned service disruptions can occur in support of periodic maintenance.

**Operational Environment Requirements -** Information about response time degradation resulting from unscheduled system outages and other events that degrade system functionality and/or performance shall be disseminated to the user community within 30 minutes of the occurrence. The notification shall include the information described in the current Automated Notification Reporting (ANR) template maintained by the VA Service Desk. The specific business impact must be noted in order for OIT to provide accurate data in the service impact notice of the ANR.

620322 **Operational Environment Requirements -** Provide a real-time monitoring solution to report agreed/identified critical system performance parameters.

**Operational Environment Requirements -** Critical business performance parameters shall be identified e.g., transaction speed, response time for screen display/refresh, data retrieval, etc. in a manner that data capture can occur to

620323

620324

620325

support metric reporting and support the OI&T performance dashboard display. If no such performance metrics are required or provided there will be no program specific Service Level Agreements (SLA) created, nor shall there be any active/real time monitoring through OI&T Performance Dashboard to provide the business owners any performance metrics.

**Operational Environment Requirements -** Notification of scheduled maintenance periods that require the service to be offline or that may degrade system performance shall be disseminated to the business user community a minimum of

48 hours prior to the scheduled event.

**Documentation Requirements -** The training curriculum provided by the applicable Program Office shall state the expected training and task completions time(s) for primary users and secondary users to become proficient at using any IT application or system that is enhanced or created as a result of this New Service

Request (NSR).

620326

620327

**Documentation Requirements -** All training curricula, user manuals, and other training tools, shall be developed and/or updated by the applicable Program Office(s) and delivered to all levels of users prior to release of any IT application or system that is enhanced or created as a result of this NSR. The curricula shall also reflect necessary updates to business processes and procedures that are changed as a result of this NSR.

**Documentation Requirements -** IT will provide the level of documentation required to support the system and maintain operations and continuity. Documentation shall represent minimal programmatic and lifecycle operations support documentation artifacts as defined by VA standards in ProPath and as required by the VA Enterprise System Engineering Lifecycle and Release Management office for sustained operations, maintenance, and support ([http://vaww.eie.va.gov/lifecycle/default.aspx)](http://vaww.eie.domain/lifecycle/default.aspx)) prior to approval by any VA change control board and release into production.

620328 **Implementation Requirements -** Technical Help Desk support for the application shall be provided for users to obtain assistance.

620329 **Implementation Requirements -** The IT solution shall be designed to comply with the applicable approved Enterprise SLA.

620330 **Implementation Requirements -** The implementation must be completed by timeframes agreed upon by both the Business Owner and OI&T.

**Data Protection/Back-up/Archive Requirements -** Based upon the criticality of

620331

620332

620333

620334

620335

620336

620337

the system, provide a back-up and data recovery process for when the system is brought off-line for maintenance or technical issues/problems.

**Data Protection/Back-up/Archive Requirements -** Data protection measures, such as back-up intervals and redundancy shall be consistent with systems categorized as mission critical (12 hour restoration).

**Data Quality/Assurance Requirements -** A monitoring process shall be provided to ensure that data is accurate and up-to-date and provides accurate alerts for malfunctions while minimizing false alarms.

**User Access/Security Requirements -** Ensure the proposed solution meets all Veterans Health Administration (VHA) Security, Privacy, and Identity Management requirements including VA Handbook 6500 (see the Enterprise Requirements section of the RTM).

**Usability/User Interface Requirements -** Adhere to good User Interface/User Centered Design (UI/UCD) principles as outlined in the Usability Appendix of the BRD.

**Privacy (Standard)** - All VA Privacy requirements will be adhered to. Efforts that involve the collection and maintenance of individually identifiable information must be covered by a Privacy Act system of records notice.

**508 Compliance (Standard) -** All Section 508 requirements will be adhered to. Compliance with Section 508 will be determined by fully meeting the applicable requirements as set forth in the VHA Section 508 checklists (1194.21, 1194.22,

1194.24, 1194.31 and 1194.41) located at: [http://www.ehealth.va.gov/508/resources\_508.htm](http://www.ehealth.domain/508/resources_508.html)l or as otherwise specified. Checkpoints will be established to ensure that accessibility is incorporated from the earliest possible design or acquisition phase and successfully implemented throughout the project.

620338 **Executive Order (Standard)** - All executive order requirements will be adhered to.

620339 **Identity Management (Standard)** - All Enterprise Identity Management

620340

620341

620342

620343

620344

620345

requirements will be adhered to. These requirements are applicable to any application that adds, updates, or performs lookups on persons.

**VE: Identity Services** - All Enterprise Identity Management requirements will be followed. These requirements are applicable to any application that adds, updates, or performs lookups on persons.

For specific guidance refer to the Identity Services BRD

[http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1385&Type=Active](http://your_srver.domain.ext/warboard/anotebk.asp?proj=1385&amp;Type=Active) Adherence to the guidance provided in these documents ensures compliance with NIST Access management policies as well as Federal Identity, Credential, and Access Management (FICAM) Guidance.

**VE: Identity and Access Management** - All Enterprise Identity and Access Control requirements will be followed. These requirements are applicable to any application that uses or manages identity information, and/or requires control of user access at any level.

For specific guidance refer to the and Enterprise Identity and Access Management

BRD (https://vaww.portal2.va.gov/sites/infosecurity/projects/Identity%20And%20Access

%20Management/SignedOfficial%20Documents/Forms/AllItems.aspx). Adherence

to the guidance provided in these documents ensures compliance with NIST Access management policies as well as FICAM Guidance.

**Terminology Services (Standard)** - Application/services shall reference Standard Data Services as the authoritative source to access non-clinical reference terminology.

**Terminology Services (Standard)** - Application/Services shall use VA Enterprise Terminology Services as the authoritative source to access clinical reference terminology.

**Terminology Services (Standard)** - Applications recording the assessments and care delivered in response to an Emergency Department visit shall conform to standards defined by the VHA-endorsed version of C 28 – Health Information Technology Standards Panel (HITSP) Emergency Care Summary Document Using Integrating the Healthcare Enterprise (IHE) Emergency Department Encounter Summary (EDES) Component.

**Terminology Services (Standard)** - Applications exchanging data summarizing a patient’s medical status shall conform to standards defined by the VHA-endorsed version of C 32 – HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component.

620346 **Terminology Services (Standard)** - Utilize nationally standardized terminology for all terms used in the solution.

**Terminology Services (Standard)** - Provide the ability to express all content using

620347

nationally recognized reference and authoritative terminology standards (e.g., Logical Observation Identifiers, Names, and Codes, Systematized Nomenclature of Medicine Clinical Terms, etc.).

620348 **Terminology Services (Standard)** - Provide the ability to record observations using standardized terms.

**Terminology Services (Standard)** - Provide the ability for users to submit a

620349

request to Standards and Terminology Services for new standardized terms (e.g., via New Term Rapid Turnaround process).

620350 **VE: HIPAA** - Computer systems shall track accounting of disclosure information

when the system is accessed by a non-VA user.

620351 **VE: HIPAA** - Computer systems shall allow for the correction or amendment of any piece of individually identifiable information.

**Interoperability** - The system shall be compliant with the interoperability

620352

620353

620354

620355

standards, specifications, and certification criteria issued by the U.S. Department of

Health and Human Services.

**EHR Certification / Meaningful Use** - The EHR shall be certified and be compliant with the standards, specifications, and certification criteria issued by the U.S. Department of Health and Human Services and maintain that certification

throughout its lifecycle. EHR Certification includes Meaningful Use requirements. The EHR shall adhere to all Meaningful Use Objectives and Standards for Eligible Providers and Eligible Hospitals (42 CFR 495.6(d)-(g)) as published or modified through the Office of National Coordinator (ONC) from the Health Information Technology (HIT) Policy (HITPC) and HIT Standards (HITSC) Committees, as well as Certification Criteria (45 CFR 170.302, 170.304, &170.306) and Standards (45 CFR 170.205, 170.207, & 170.210).

**Patient Driven Care and Care Coordination** - The system shall have the capability of incorporating patient self-entered data in order to provide context- specific care. This may include results of home monitoring and patient-reported functional outcomes (e.g., Veterans RAND 12-Item Health Survey, Functional Independence Measurement, Patient Health Questionnaire-9, Patient Reported Outcomes Measurement Information System, etc.) provided as structured documents that use structured encoded data elements. The system shall support self-entered data by authenticated patients and clearly identify this as patient- entered data so that providers may consider this in their review and interpretation. Authenticated and labeled self-entered data will be available across applications. The system must capture in standard format (e.g., Health Level 7 Clinical Document Architecture) the plan of care (including individualized treatment considerations and goals) which will be shared with the patient and members of the treatment team.

The system shall generate a summary record that meets Meaningful Use standards. The system shall have the capability to generate, at all user-defined

levels, a list and summary of all patients meeting defined criteria (e.g., diagnosis of

diabetes), for purposes of panel management and care coordination. The system shall be compliant with and support the criteria of the National Committee for

Quality Assurance (NCQA) for Patient Centered Medical Home, Level 3 recognition

program.

**Business Intelligence / Analytics** - The system requires the capability to generate aggregate reports as needed (e.g., Meaningful Use Quality Measures, quality monitoring, performance accountability, research initiatives, etc.), with the ability to strip personally identifying information. Structured clinical data will be collected according to recognized standards within Meaningful Use (SNOMED, LOINC, RxNorm, etc.). The system requires a variety of reporting tools (e.g., patient-centric, facility-centric, region/service-centric, enterprise-level, and population-based, etc.). These reporting tools shall be relevant, adaptable and easily used by the end-user. The reports generated and their associated data shall also be easily exportable. The system requires the capability to identify, track, and report aggregate performance stratified by key patient characteristics such as gender, race/ethnicity, Benefit Category, diagnostic categories (e.g., mental illness diagnoses, etc.) and other factors, in order to track health disparities and address

the needs of vulnerable populations. System tools may include predictive modeling.

It is imperative that impact on workflow (both system performance and healthcare team processes and outcomes) is tracked when modifications are made to the system.

620356 **HIPAA Security Rule** - Information system shall implement reasonable and appropriate security measures to reduce risk.

620357 **HIPAA Security Rule** - Information system shall implement reasonable and appropriate security measures to minimize vulnerabilities.

620358 **HIPAA Security Rule** - Information systems shall validate a user's right of access

(authorization) to electronic Personal Health Information (ePHI).

620359 **HIPAA Security Rule** - Information system shall monitor user log-in attempts.

620360 **HIPAA Security Rule** - Information system shall notify user of invalid log-in attempts.

620361 **HIPAA Security Rule** - Information systems shall enforce a limit to the number of consecutive invalid user log-in attempts during a specified time period.

620362 **HIPAA Security Rule** - Information systems shall log user log-in attempts.

620363 **HIPAA Security Rule** - Information system shall provide capability to create passwords.

620364 **HIPAA Security Rule** - Information system shall provide capability to change passwords.

620365 **HIPAA Security Rule** - Information system shall safeguard passwords.

620366 **HIPAA Security Rule** - Information system shall implement an electronic mechanism that allows only authorized entities access to ePHI.

620367 **HIPAA Security Rule** - Information system shall assign a unique name and/or number to identify a user.

620368 **HIPAA Security Rule** - Information system shall use a unique name and/or number to track a user.

620369 **HIPAA Security Rule** - Information system shall implement a process to allow access to necessary ePHI during an emergency.

620370 **HIPAA Security Rule** - Information system shall implement electronic mechanism to terminate an electronic session after a predetermined time of inactivity.

620371 **HIPAA Security Rule** - Information system shall implement mechanism to encrypt and decrypt ePHI.

620372 **HIPAA Security Rule** - Information system shall record activity in information systems that contain or use ePHI.

620373 **HIPAA Security Rule** - Information system shall examine activity in information systems that contain or use ePHI.

620374 **HIPAA Security Rule** - Information system shall implement an electronic mechanism to protect ePHI from improper alteration.

620375 **HIPAA Security Rule** - Information system shall implement an electronic mechanism to protect ePHI from improper destruction.

620376 **HIPAA Security Rule** - Information system shall implement electronic mechanism to verify that ePHI has not been altered in an unauthorized manner.

620377 **HIPAA Security Rule** - Information system shall implement electronic mechanism to verify that ePHI has not been destroyed in an unauthorized manner.

620378 **HIPAA Security Rule** - Information system shall implement electronic mechanisms to authenticate a user.

620379 **HIPAA Security Rule** - Information system shall implement mechanisms to guard

against unauthorized access to ePHI during transmission.

620380 **HIPAA Security Rule** - Information system shall implement mechanisms to verify that electronically transmitted ePHI is not improperly modified during transmission.

620381 **HIPAA Security Rule** - Information system shall implement mechanisms to encrypt ePHI during transmission.

620382 **HIPAA Security Rule** - Information system shall implement electronic mechanisms to authenticate an interfacing system or other entity.

620383 **HIPAA Security Rule** - Information system shall implement mechanisms to encrypt

ePHI at rest on mobile devices or removable electronic media.

**2.8. Features**

|  |  |  |  |
| --- | --- | --- | --- |
| ID | FEATURE Name | FEATURE Input | FEATURE Output |
| F1 | Send Laboratory Ordering Provider contact information  To be determined if part of scope | Provider Phone Number (New Person File #200; Office Phone Field #.132)  Provider Digital Pager  Number (New Person File  #200; Digital Pager Field  #.138)  Provider Voice Pager  Number (New Person File  #200; Voice Pager Field  #.137) | Electronic message transmission to Autoverification System with additional information. |
| F2 | Receive Laboratory Result with indication of results Autoverified or verified by a Technologist | Electronic message transmission from Autoverification System with additional information | Patient result viewable in CPRS and VistA Laboratory with |
|  | Develop a master auto release switch |  | LA7UI AUTO RELEASE MASTER. Its main function would be as a “kill switch”. Namespace would indicate Lab  Automated (LA) Universal Interface (UI)  Auto Release. This  would provide granularity in case in the future auto release is also expanded to include reference lab results (LEDI). |

**3. Applicable Standards**

**4. Interfaces**

Health Level 7 (HL7) version 2.2 messaging currently used in VistA Legacy Laboratory system

Universal Interface capability.

**4.1. Communications Interfaces**

*TBD*

**4.2. Hardware Interfaces**

*TBD*

**4.3. Software Interfaces**

VistA Laboratory Universal Interface

• HL7 ORM Messages will be modified to include provider contact information, see SDD.

• HL7 ORU Messages will be modified to include indicator of ‘Autoverified’ results.

*.*

**4.4. User Interfaces**

Existing user interface for VistA Legacy Laboratory Auto Instrument functionality, existing VistA Legacy Laboratory system, and existing CPRS.

**5. Legal, Copyright, and Other Notices**

The legacy VistA Laboratory software runs within the VistA architecture on the VA’s network. The following warning is issued during the log in process:

“This U.S. Government computer system is for official use only. The files on this system include Federal records that contain sensitive information. All activities on this system may be monitored to measure network performance and resource utilization; to detect unauthorized access to or misuse of the system or individual files and utilities on the system, including personal use; and to protect the operational integrity of the system. Further use of this system constitutes your consent to such monitoring. Misuse of or unauthorized access to this system may result in criminal prosecution and disciplinary, adverse, or other appropriate action.”

**6. Purchased Components**

None, for VistA Patch component.

**6.1. Defect Source (TOP 5)**

Not Applicable.

**7. User Class Characteristics**

Laboratory Medical Technologists, Laboratory Information Managers, Information Technology Support Staff, and physicians, nurses, pharmacists, as well as other care givers who use patient results in order to treat and/or care for patients.

**8. Estimation**

**Project Software Functional Size and Size-Based**

**Effort and Duration Estimate**

The functional size of the project is 42 FP (Function Points).

**Application**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item** | **A** | **B** | **C** | **D** | **E** | **Total** |
| **Counted**  **Function Points** |  |  |  |  |  |  |
| **Estimated Scope**  **Growth** |  |  |  |  |  |  |
| **Estimated Size at**  **Release** |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Size-Based Effort Estimates** | **Labor Hours** | **Probability** |
| **Low-Effort Estimate – With indicated probability, project will consume no more than:** | 910 | 50% |
| **High-Effort Estimate – With indicated probability, project will consume no more than:** | 1680 | 75% |

|  |  |  |
| --- | --- | --- |
| **Size-Based Duration Estimates** | **Work Days** | **Probability** |
| **Low-Duration Estimate – With indicated probability, project will consume no more than:** | 73 | 50% |
| **High-Duration Estimate -- With indicated probability, project will consume no more than:** | 122 | 75% |

**Figure 1: Cumulative Probability (“S-curve”) Chart**

**Cumulative Probability Curve (project effort)**

FP Estimate Simulator v13

100 %

90%

- ---

...,;

>

.CI

**.CI**

D..

70%

30%

/

/*v*

/';

i

/

I

/

io"""

./\_

I I

20%

10%

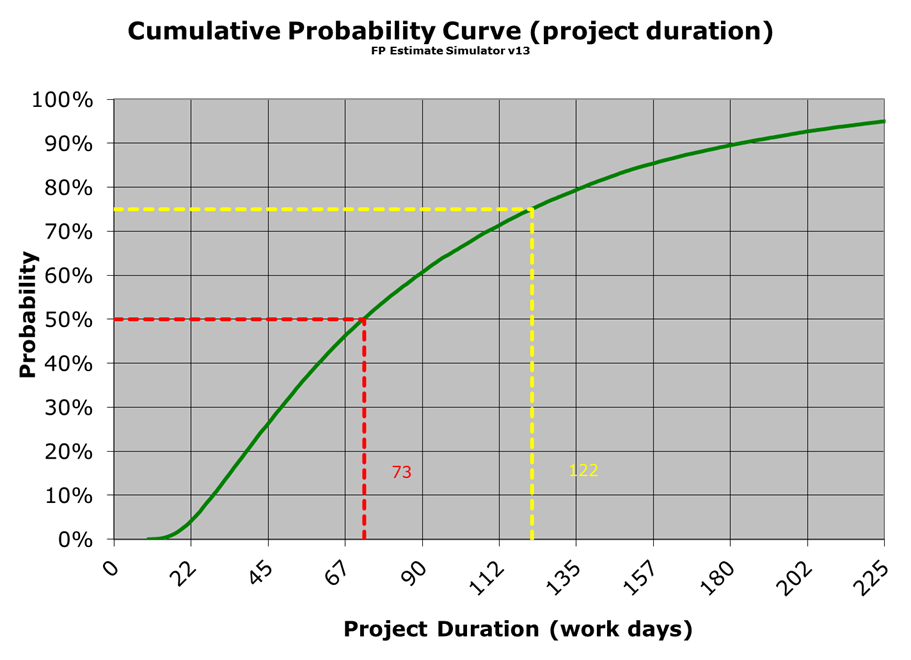
()

*v* I uo

/ :I

*j* I

**Total Project Effort (hours)**



**9. Approval Signatures**

Signed:

, Integrated Project Team (IPT) Chair/ Project Manager

Signed:

, Business Sponsor

Signed:

, OI&T IT Program Manager