

Department of Veterans Affairs

Bar Code Enhancement – Positive Patient Identification

Increment 2 – Pyxis® Transfusion Verification

**Vista Applications / VBECS Interfacing with a COTS Blood Administration
Point of Care System**

System Design Document



April 2014

Version 1.0

Revision History

Date	Version	Description	Author
September 16, 2013	0.01	Modified all sections to reflect current Transfusion Verification information.	[REDACTED]
Oct 14, 2013	0.02	Checked into SharePoint	[REDACTED]
Nov 25, 2013	0.03	Added material on recovering from manual operations, accepted all changes. Responded to and deleted all comments.	[REDACTED]
Jan 26, 2014	0.04	Responded to reviews from DCO and SDE. Added new material, added reference to SDE SDD. Added explanatory material in response to DCO remarks on figures 10 and 12 and table 13. Added two comments which must be addressed by SDE prior to finalization of the document.	[REDACTED]
Jan 27, 2014	0.05	Technical writer review.	[REDACTED]
March 17, 2014	0.06	Added material on logical design , physical design and security from the Production Operations Manual	[REDACTED]
March 17-18, 2014	0.07	Technical writer review.	[REDACTED]
March 18, 2014	0.08	Peer Review.	[REDACTED]
April 28, 2014	1.0	Addressed technical and non-technical comments from the peer review.	[REDACTED]
May 10, 2014	1.1	Added material on High Availability, addressed more comments	[REDACTED]

Table of Contents

1.	Introduction.....	1
1.1.	Purpose of this document	1
1.2.	Identification	2
1.3.	Scope	2
1.4.	Relationship to Other Plans.....	5
1.5.	Methodology, Tools, and Techniques	5
1.6.	Policies, Directives and Procedures.....	6
1.7.	Constraints	7
1.7.1.	High-Level Design Constraints.....	7
1.7.2.	Time Management Design Constraints.....	8
1.7.3.	CareFusion Hand-held Device Constraints.....	8
1.7.4.	VA System Compatibility Constraints.....	8
1.7.5.	Design Trade-offs	8
1.8.	User Characteristics.....	9
1.8.1.	User Problem Statement	9
1.8.2.	User Objectives.....	9
2.	Background	11
2.1.	Overview of the System	11
2.1.1.	Architectural Overview of the System	11
2.1.2.	Deployment Overview.....	15
2.2.	Overview of the Business Process	15
2.3.	Business Benefits.....	18
2.4.	Assumptions and Constraints	18
2.4.1.	Design Assumptions.....	18
2.4.2.	Design Constraints.....	19
2.4.2.1.	Constraints Expressed as Business Rules.....	19
2.4.2.2.	Constraints Expresses as System Specifications	19
2.4.2.3.	VistA Constraints	19
2.4.2.4.	CareFusion Constraints	20
2.5.	Overview of the Significant Requirements	20
2.5.1.	Significant Interfacing Requirements	20
2.5.2.	Workload and Capacity Requirements.....	22
2.5.2.1.	Current State of Workload Assessment.....	22
2.5.2.2.	Initial Capacity Plan	24
2.5.2.3.	Capacity Planning Concerns	24
2.5.3.	Operational Requirements.....	25

2.5.4.	Overview of the Technical Requirements	28
2.5.4.1.	Multi-Divisional Specifications.....	29
2.5.4.2.	Performance Specifications.....	29
2.5.4.3.	Quality Attributes Specifications.....	29
2.5.4.4.	Reliability Specifications.....	29
2.5.4.5.	Usability Specifications	29
2.5.5.	Overview of the Security and Privacy Requirements	29
2.5.5.1.	Wireless Security	32
2.5.6.	System Criticality and High Availability Requirements	32
2.5.7.	Special Device Requirements	33
3.	Conceptual Design	34
3.1.	Conceptual Application Design.....	34
3.1.1.	Application Context.....	34
3.1.2.	Application Locations	38
3.1.3.	Application Users	39
3.2.	Conceptual Data Design	39
3.2.1.	Project Conceptual Data Model	39
3.2.2.	Conceptual Database Information.....	40
3.3.	Conceptual Infrastructure Design	40
3.3.1.	System Criticality and High Availability	41
3.3.2.	Special Technology	44
3.3.3.	Conceptual Overview of Physical Infrastructure	44
4.	System Architecture.....	45
4.1.	Hardware Architecture	49
4.1.1.	Virtual Server Configuration	50
4.1.2.	System Deployment Logical Overview and server Side Deployment Overview	53
4.1.3.	Physical System Deployment Overview	54
4.2.	Software Architecture	60
4.3.	Communications Architecture.....	66
5.	Data Design.....	69
5.1.	Database Management System Files	69
5.1.1.	Site-Specific Database.....	69
5.1.2.	Scripts required to connect the CFTV application and database servers to VISTA	70
5.1.3.	Scripts required to connect the CFTV application and database servers to VISTA	70
5.1.4.	Procedure for linking an application server to its site-specific database	70

5.2.	Non-Database Management System Files.....	71
6.	Detailed Design	72
6.1.	Hardware Detailed Design.....	72
6.2.	Software Detailed Design.....	76
6.2.1.	VISTA-PIMS ADT	77
6.2.2.	VISTA CPRS – TIU.....	77
6.2.3.	Vista Patient Orders	78
6.2.4.	Vista Blood Establishment Computer System.....	78
6.2.5.	CareFusion Pyxis TV System Server Software – Interface Package.....	79
6.2.6.	CareFusion Pyxis TV System Server Software – Management Console	80
6.2.7.	CareFusion Pyxis TV System Software –Windows Client Software.....	80
6.2.8.	CareFusion Pyxis TV System Software –EDA Controller	80
6.2.9.	CareFusion Pyxis TV System Software – Web Services	81
6.2.10.	Detailed Design of the BCE Application Server	82
7.	External Interface Design.....	86
7.1.	Interface Overview and Data Transfer	86
7.2.	Interface Requirements	88
7.2.1.	VISTA Interface Requirements	88
7.2.2.	VBECS Interface Requirements.....	89
7.2.2.1.	Requirements for Messages Inbound to VBECS	89
7.3.	Hardware Interfaces	97
7.4.	Software Interfaces	98
7.5.	Interface Detailed Design	98
7.5.1.	Interface Software Dependencies	99
7.5.2.	ADT HL7 Interface Elaboration	99
7.5.3.	ADT HL7 Protocols	99
7.5.4.	TIU HL7 Interface Elaboration.....	107
7.5.5.	Vitals Remote Procedure Calls Interface Elaboration	108
7.5.6.	Software Product Security	114
7.5.6.1.	Mail Group.....	114
7.5.6.2.	Archiving	115
7.6.	Human-Machine Interface	116
8.	System Integrity Controls.....	117
8.1.	BCE-PPI System Integrity.....	117
8.2.	CareFusion Pyxis TV Access Control	124
9.	Requirements Traceability Matrix	127
10.	Packaging and Installation	127

11. Design Metrics	127
12. Required Technical Documents	127
Appendix A – TIU Note with Vital Signs.....	130
Appendix B – Acronyms and Definitions	133
Appendix C - Glossary of Terms.....	136
Appendix D – References.....	141
Appendix E – Data Elements for the VBECS to CFTV Interfaces	144
Appendix F - Approval Signatures	150

List of Figures

Figure 1: BCE-PPI CF Patient Point of Care (PPOC) End State Overview	12
Figure 2: High-Level Conceptual Diagram of the BCE-PPI Increment 2 BAPOC System	13
Figure 3: BCE-PPI Increment II TV High-Level Communication Architecture	14
Figure 4: Overview of the Business Process for Blood Administration	16
Figure 5: Basic transfusion workflow (to be standardized by BCE-PPI Increment 2)	17
Figure 6: High-level Overview of Bar Code Enabled Transfusion Verification	35
Figure 7: High-level architecture	36
Figure 8: BCE PPI TV Message Context Diagram	37
Figure 9: Conceptual Overview of Physical Architecture (Host Hardware)	44
Figure 10: CFTV VA System Architecture	45
Figure 11: High-level system architecture for the BAPOC system	47
Figure 12: Interfaces depicted at a high-level (e.g. HL7)	48
Figure 13: BCE-PPI Deployment Diagram (Logical System View)	54
Figure 14: BCE-PPI Increment 2 Software Component Architecture	63
Figure 15: Communication Architecture	67
Figure 16: BCE-PPI Expansion VBECS HL7 Messaging Context Diagram	68
Figure 17: CFTV Production Application Servers Hardware Specification	73
Figure 18: BCE-PPI Production SQL Server Types	75
Figure 19: BCE-PPI Increment II Overall System Architecture and Interface Identification	76
Figure 20: CFTV Management Console Main Page Showing Software Versions	82
Figure 21: CFTV Application Server Components and Relationships	84
Figure 22: BCE-PPI Increment II Interface Identification Diagram	86

List of Tables

Table 1: Preferred and Alternate Names for COTS Applications for BCE-PPI	3
Table 2: Preferred and Alternate Names for COTS System Components	4
Table 3: VA system's overall specifications as they pertain to the interface with BAPOC COTS application	20
Table 4: Detailed Interface Requirements	21
Table 5: Workload Requirements	23
Table 6: Operational Requirements	25
Table 7: Security Requirements.....	30
Table 8: User Authorization and Authentication roles	31
Table 9: CareFusion Pyxis TV Security Roles and Corresponding VistA Access	31
Table 10: Application Locations	38
Table 11: Application Users	39
Table 12: Recommended minimum system requirements	50
Table 13: Required Patch Levels	51
Table 14: VM Template Configuration for the CFTV Application Server.....	52
Table 15: Physical Distribution of the CFTV (COTS) Server VM's for BCE-PPI Increment 2	57
Table 16: Physical Configuration of Guest VM's for BCE-PPI Increment 2	58
Table 17: Increment 1 COTS Software Installed with Corresponding VA Interfaces.....	60
Table 18: VistA and VBECS required patch levels	61
Table 19: Component Abbreviations and Names	65
Table 20: VISTA-PIMS ADT	77
Table 21: VISTA- TIU.....	78
Table 22: VistA Patient Orders.....	78
Table 23: Vista Blood Establishment Computer System.....	79
Table 24: CareFusion Pyxis TV System Server Software – Interface Package.....	79
Table 25: CFTV BAPOC System Server Software – Management Console	80
Table 26: CFTV BAPOC System Software –Windows Client Software	80
Table 27: CFTV BAPOC System Software –EDA Controller	81
Table 28: COTS BAPOC System Software – Web Services.....	81
Table 29: BCE-PPI Increment II Interface Summary with HL7 Versions	87
Table 30: VBECS HL7 Processing.....	90
Table 31: VBECS HL7 Processing.....	93
Table 32: Software Patches and Dependencies	99
Table 33: Subscriber Protocol Names	99
Table 34: VistA Authentication RPC's	Error! Bookmark not defined.
Table 35: Mail Group Description.....	115
Table 36: EAS Regression Test Results for CFTV Web Application from the 2/7/2014 Report.....	119
Table 37: CFTV Web Application findings that are now closed.....	124
Table 38: CFTV Security Roles and Corresponding VistA Access	124
Table 39: Acronyms and Definitions.....	133
Table 40: Glossary of Terms	136

1. Introduction

The Bar Code Expansion – Positive Patient Identification (BCE-PPI) Blood Administration project is a commercial-off-the-shelf (COTS) system integration effort which will implement the CareFusion (CF) Point of Care (POC) system in the VA. When implemented, the integrated system will be composed of COTS software components developed for the Veterans Administration (VA) by MicroTech/CF, and modified versions of existing VA software which will be deployed as part of the Veterans Integrated System of Technological Architecture (VistA).

Increment 2 of the BCE-PPI project seeks to deploy a COTS Blood Administration Point of Care (BAPOC) system that will interface with VistA and the Veterans Blood Establishment Computer System (VBECS). This POC system will allow users to positively identify patients using bar code functionality as well as automate some of the documentation required during a transfusion event

The MicroTech/CF development team will assist in the deployment of the Pyxis® Transfusion Verification (TV) application as part of the overall system integration. In addition, increment 2 will deploy the CareFusion Pyxis Wireless Medication Administration (WMA) and Pyxis Nurses Data Collection (NDC) applications, which were validated for deployment during increment 1.

1.1. Purpose of this document

The primary purpose of the Product Development (PD) SDD is to present the software design for the integrated system to be delivered as increment 2. The design described here will be used to track progress and to verify that the vendor has satisfied all the requirements identified by the stakeholders. It will also be used to identify the changes that need to take place on the VA side to successfully integrate the COTS products into the VA architecture and business processes.

It is important to understand that BCE-PPI increment 2 currently has two SDDs, which we will refer to as the SDE SDD and PD SDD respectively. The SDE SDD is a Visio document prepared by the Systems Design and Engineering group. The SDE SDD was prepared to address the specific requirements of the System Engineering Design Review (SEDR). Currently the SEDR is an internal review performed by SDE Engineers. Both the SEDR and the SDE SDD are focused on the hardware, network and deployment architecture of the system. The SDE SDD by its nature does not address many facets of the system design, those facets are best addressed by the Product Development Team and we have done our best to address them in this document.

The SDE SDD is titled, **VA_Enterprise Systems Engineering (ESE)_BCE-PPI_DESIGN_vA.0.5.vsd**, but it has the legend BCE-PPI System Design on the Title Page. The document is available in the BCE-PPI SharePoint at the link below:

[http://\[REDACTED\]](http://[REDACTED])

In this document and other BCE-PPI Increment 2 documents references to the SDD (with no qualification) refer to the PD SDD.

1.2. Identification

The following systems are included in the integrated design for the Blood Administration Point of Care system and are addressed in this design document.

- VistA CPRS / TIU
- VistA Vitals
- VistA PIMS Admission Discharge Transfer (ADT)
- VistA Remote Procedure Call (RPC) Broker
- VBECS
- CareFusion Pyxis® Transfusion Verification (a COTS Product)
- CareFusion Interface Package (CFIE) (a COTS Product)
- CareFusion Management Console (CFMC) (a COTS Product)

The requirements that the integrated design must meet are detailed in the Requirements Specification Document (RSD) for increment 2, which is titled:

BCE-PPI Increment 2 VistA Applications / VBECS Interfacing with a COTS BAPOC System.

The RSD can be found on the project SharePoint site at the following link:

[http://\[REDACTED\]](http://[REDACTED])

1.3. Scope

The scope of the BCE PPI Blood Administration Increment 2 Project is to extend the barcode enablement provided by the CF Point of Care system to blood administration. This includes procurement and installation of the required COTS components and development of the interfaces between the COTS products and the VistA packages involved in patient identification and blood administration.

This SDD details the design of the integrated system and shows how that design will meet the technical and stakeholder functional requirements. It also details what the combined vendor and VistA systems will need to deliver (in terms of hardware, software and interfaces) in order to achieve the successful deployment and sustainment of BCI-PPI Blood Administration.

After full deployment, clinicians will use the integrated system for Blood Components Administration, using an Enterprise Digital Assistant (EDA), and/or a wired or wireless workstation with an integrated barcode scanner to match patients and blood products reliably using barcode technology. This PD SDD describes how the integrated software system will be designed to meet the needs of those clinicians.

1.4. Standard Terminology

We have made every effort to stick to a standard terminology for the COTS products and system components in all of the documentation for BCE-PPI Increment 2. However, this is easier said than done for several reasons:

1. Standard terminology has come very late in the increment and using the latest standard terms would require a very large effort to retrofit all of the existing documents.
2. The standard terminology the COTS vendor uses for its own products and servers has also been changing over time. For example, many of the vendor user guides for CareFusion Pyxis Transfusion Verification refer to CFTV as the product and CFTV servers for the machines hosting the software.
3. A dose of common sense is also helpful here. It should be understood that a server which is called a CFTV Application Server doesn't have to host just the TV application. It can also host CareFusion WMA, NDC and SCV applications. This simple assumption avoids the need to modify dozens of documents and hundreds of diagrams to use the currently preferred term, which is BCE Application Server. Note that CFTV, CFTV Server, CFTV Application Server and CFTV Database Server are used very frequently and interchangeably in all of the COTS vendor manuals.

Table 1 and 2 should serve as a useful guide in fixing the meaning of application and component names for all of the BCE-PPI Increment 2 documentation.

Table 1: Preferred and Alternate Names for COTS Applications for BCE-PPI

Application	Preferred Term	Alternate Term	Preferred Acronym	Alternative Acronym
COTS Transfusion Verification application	CareFusion Pyxis Transfusion Verification	CareFusion Transfusion Verification	CFPTV	CFTV
COTS Wireless Medication Administration application	CareFusion Pyxis Wireless Medication Administration	CareFusion WMA	WMA	None
COTS Nurses Data Collection application	CareFusion Pyxis Wireless Medication Administration	CareFusion NDC	NDC	None

Application	Preferred Term	Alternate Term	Preferred Acronym	Alternative Acronym
COTS Specimen Collection Verification application	CareFusion Pyxis Specimen Collection Verification	CareFusion SCV	SCV	None

Table 2: Preferred and Alternate Names for COTS System Components

Component	Preferred Term	Alternate Term	Preferred Acronym	Alternative Acronym
Virtual Machine hosting all CareFusion Pyxis applications for the BCE-PPI server	BCE Application Server BCE App Server	CFTV App Server	BCEAPP	None
Virtual Machine (VM) hosting all CareFusion Pyxis Databases	BCE Database Server BCE SQL Server	CFTV Database Server	BCESQL	None
Database hosting site-specific data for the CareFusion Pyxis TV application	BCE site-specific database	CFTV Site-specific database Note that other databases may be required for other Pyxis applications, e.g SCV so there is a sense in which CFTV site-specific database is preferable.	CFTVDB	None

We have endeavored to use the preferred terms in the verbiage in this document and the POM. However, the diagrams still use the older terminology as does some of the text.

1.5. Relationship to Other Plans

This PD SDD is related to the following project documents for increment 2:

- Project Management Plan (PMP)
- Requirements Specification Documents (RSD)
- Master Test Plan (MTP)
- Test Cases and Test Scripts
- Deployment Plan
- Product Operations Manual (POM)
- Installation Guide: MJCF (VistA) Installation Guide, CareFusion Transfusion Verification (CFTV) Installation Guide, EDA Device Configuration Manual
- Operations Acceptance Plan (OAP)
- Software Configuration Management Procedures (SCMP)
- SDE SDD (prepared by SDE)

These documents are available in the BCE-PPI SharePoint site. References are provided in Appendix D.

1.6. Methodology, Tools, and Techniques

The VA Product Development (PD) division has standardized the development tool set of the following tools in order to provide access control, consistency of information, and to help development teams successfully complete their tasks:

- Rational® RequisitePro® (Requirements)
- Rational® ClearQuest® (Change requests, risk tracking, issue tracking)
- Rational® Quality Manager (Test Scripts / Test Cases)
- Rational® Clear Case® (Version Control)

The project management methodology used on this project is PMAS/ProPath, the VA Standard. The PMAS/ProPath methodology is also being used for software development. Change and Configuration Control Methods are described in the Configuration Management section of the Project Management Plan (PMP). That document describes the methods used for issue management, change management, build management, release management and deployment. The procedures used to manage testing are described in the MTP and the methodology which governs deployment is described in the deployment plan.

Because of the importance of change management in an application which is directly involved in patient care, we provide a brief sketch of change management procedures here:

1. Requested changes are captured in ClearQuest (CQ) in the form of a Change Request (CR).

2. A National Service request (NSR) is another way of proposing changes to existing software and getting the software upgraded or replaced.
3. The procedures for making entering change requests in ClearQuest are provided in the Project Management Plan in the Change Management section).
4. The procedures for filing a NSR are provided in the POM.

The composition of the Change Control Board and the agreed-upon procedures for approving, rejecting or deferring a requested change are spelled out PMP.

1.7. Policies, Directives and Procedures

The development team will adhere to all applicable federal and VA policies for this project to produce software that is compliant with standards for patient safety, patient privacy, data and system security and user accessibility. The relevant policies governing project management and software development include:

- 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
- Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
- FIPS Pub 201, “Personal Identity Verification of Federal Employees and Contractors,” March 2006
- Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
- 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
- 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
- Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program,” May 18, 2007
- VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
- 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
- Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
- An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
- Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
- Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
- VA Directive 6500, “Information Security Program,” August 4, 2006
- VA Handbook 6500, “Information Security Program,” September 18, 2007
- VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
- VA Handbook 6500.2, “Management of Security and Privacy Incidents,” June 17, 2008.
- VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008.
- VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
- VA Handbook 6500.6, “Contract Security,” March 12, 2010

- PMAS portal (reference PWS References –Technical Library at [https://\[REDACTED\]/](https://[REDACTED]/))
- OIT ProPath Process Methodology (reference PWS References –Technical Library and ProPath Library links at [https://\[REDACTED\]](https://[REDACTED]) NOTE: In the event of a conflict, OIT ProPath takes precedence over other processes or methodologies.
- Technical Reference Model (TRM) (reference at [http://\[REDACTED\]](http://[REDACTED]))
- National Institute Standards and Technology (NIST) Special Publications
- VA Directive 6508, VA Privacy Impact Assessment (PIA), October 3, 2008
- VA Directive 6300, Records and Information Management, February 26, 2009
- VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
- EIA-649A, “National Consensus Standard for Configuration Management”
- Health Insurance Portability and Accountability Act of 1996
- Health Insurance Portability and Accountability Act of 1996 (Privacy Rule) effective October 15, 2002
- Health Insurance Portability and Accountability Act of 1996 (Security Rule) effective April 21, 2003
- Privacy Act of 1974, (5 U.S.C. 552a eq. seq)
- Clinger-Cohen Act of 1996, 40 U.S.C. 1401 et seq.
- Public Law 104-113: National Technology Transfer and Advancement Act of 1995. 104th Congress, March 7, 1996
- OMB Circular NO. A-130: Management of Federal Information Resources, November 28, 2000

1.8. Constraints

1.8.1. High-Level Design Constraints

The constraints imposed on the design by specifications found in the RSD are detailed in section 2.4.2 of this document in the Design Constraints section. For convenience, the key design constraints are highlighted here:

- The Pyxis® TV product must meet 100% of the documented requirements for each increment release.
- The project schedule, scope, and budget are dependent on the PMAS submission, review and approval process.
- All functionality in the Pyxis® TV product software shall be fully compliant with the required standards.

Since the heart of the Blood Administration Point of Care solution is a COTS product, these constraints primarily apply to the vendor. In essence and taken together, they constrain the vendor to full compliance with the VA Software Development Life Cycle (SDLC) policies and procedures including release preparation, full testing and test approval, and compliance with VA Quality Assurance standards. In particular, the vendor is constrained to full participation in the delivery of all of the required PMAS documents.

1.8.2. Time Management Design Constraints

Deploying the CF software to a set of Virtual Machines (VMs) located at remote data center makes time management an issue because the server and its clients are no longer guaranteed to be in the same time zone.

1.8.3. CareFusion Hand-held Device Constraints

The EDA device is the core of the Pyxis® TV system and ensuring that the EDAs selected are compatible with the CFTV servers is a design constraint.

The vendor recommends the Motorola MC75AO EDA because of its scanning capability, portability, and hardware-level wireless security compliance to the FIPS 140-2 data exchange standard, in accordance with VA wireless security policy. The MC75AO is the only EDA device meeting VA TRM_0067OP-EDA requirements that is constructed of healthcare-approved plastics. Healthcare-approved plastics housings are a VA requirement for compatibility with cleaning and disinfecting solutions used at VA facilities.

1.8.4. VA System Compatibility Constraints

The VA Systems in the overall solution need to be compatible with the CareFusion product interface as defined in the Interface Specifications in this document (section 7). The BCE-PPI system interfaces with both VBECS and VistA. If changes are made to the interface or operation of VBECS, VistA HL7, TIU, Vitals or ADT there may need to be changes on the CareFusion side. Modifications to the CareFusion software may require corresponding modifications to VA systems. These modifications will be made using the patch mechanism already in place for VBECS, VistA, etc.

The specific patch levels required for the VA systems to support integration with the CareFusion software are spelled out later in this document.

1.8.5. Design Trade-offs

For BCE-PPI Increment 2, the design trade-offs involved in implementing a COTS solution were carefully considered during the procurement. Any COTS acquisition trades the (presumably) lower development costs for purchased software against the increased integration costs. For most COTS products the support costs are higher because vendor support personnel must be added to the support team and additional levels must be added to the all of the issue escalation procedures.

One example of such a trade-off is the inclusion of information on setting values in configuration files in the PD SDD. If all configuration changes are to be made by vendor personnel then there is no need to include configuration file information in the PD SDD.

It has been determined that the VA team will be responsible for capturing and distributing configuration information for the BCE server software. However, that information will be captured in the various CFTV installation and configuration guides. The following guides already exist.

1. CFTV Application Server Installation Guides – This guides provide the information required to install CFTV application software on a clean CFTV application server VM created from a “bare metal” template.

2. CFTV Database Server Installation Guide - This guide provides the information required to install CFTV database software on a clean CFTV Database Server VM created from a “bare metal” template. It also describes how to create CFTV site-specific databases.

These Install Guides are published in the BCE-PPI SharePoint site. References are available in appendix D.

The following guides are tentatively scheduled but they may not be produced, because if a decision to build all CFTV Application and Database Servers “from scratch” is made then there will be no cloning and all CFTV servers will be created by performing software installs using the CFTV Install Guides.

3. CFTV Replication Guide – If cloning is used, this guide provides the information required to create a working CFTV server by cloning a ‘gold template’, meaning a VM image which has been created from a working CFTV VM.
4. CFTV Configuration Guide – If cloning is used, this guide provides the information required to configure a replicated (cloned) CFTV VM for use at a specific site.

1.9. User Characteristics

The users of the Blood Administration portion of the BCE PPI system are trained clinicians who administer blood products at VAMC’s. This includes transfusionists and nurses.

While these users are proficient in the use of Vista desktop applications, specific training on both the CareFusion TV desktop/laptop client programs and the CareFusion TV EDA devices will be provided so users can get the most out of the bar code software when delivering and accounting for blood products.

1.9.1. User Problem Statement

There is currently no automated process to match the patient to the blood product through the use of positive patient identification at the point of care. Additionally, the official patient record for the transfusion is currently documented manually using VA Blood Transfusion Record Form (BTRF). BCE-PPI increment 2 will address these issues by providing an automated process to match patients and blood products using barcode technology and by providing automated updates to the patient records when transfusions are administered.

1.9.2. User Objectives

The high-level project objectives for the BCE PPI increment 2 are as follows:

- Increase the accuracy of patient identification at the point of care.
- Reduce the probability of adverse events due to misidentification when administering blood products.

The objectives of BCE-PPI increment 2 TV will be achieved as steps toward reaching the high-level goals listed below:

1. Increase accuracy of patient identification for an episode of care and reduce the incidence of adverse events due to misidentification.
2. Reduce patient misidentification when specimen labeling for clinical laboratory.

3. Reduce patient misidentification when specimen labeling for anatomic pathology.
4. Reduce wrong blood product administration.
5. Reduce redundant and inefficient documentation for blood administration.
6. Increase patient safety (decreased morbidity and mortality).

This PD SDD for increment 2 is intended to describe the software design for using barcodes to reduce patient misidentification during blood product administration (meeting objectives 1, 4, 5, and 6). This project will help VHA meet the following Joint Commission's National Patient Safety Goals:

2010 (NPSG) 01.01.01: Use at least two patient identifiers when providing care, treatment and services,
2010 (NPSG) 01.03.01: Eliminate transfusion errors related to patient misidentification.

2. Background

The BCE-PPI Blood Administration effort is the second increment of the larger BCE-PPI project. Increment 2 is an effort to make blood product administration more accurate by requiring clinicians to perform actions at the point of care using barcodes and automated technology to read barcodes. The main purpose of Increment 2 is to reduce errors associated with inaccurate patient / blood product matches at the point of care by matching the patient barcode with the blood product barcode. Other increments in the BCE PPI will apply barcode technology to other aspects of patient care as discussed in the introduction.

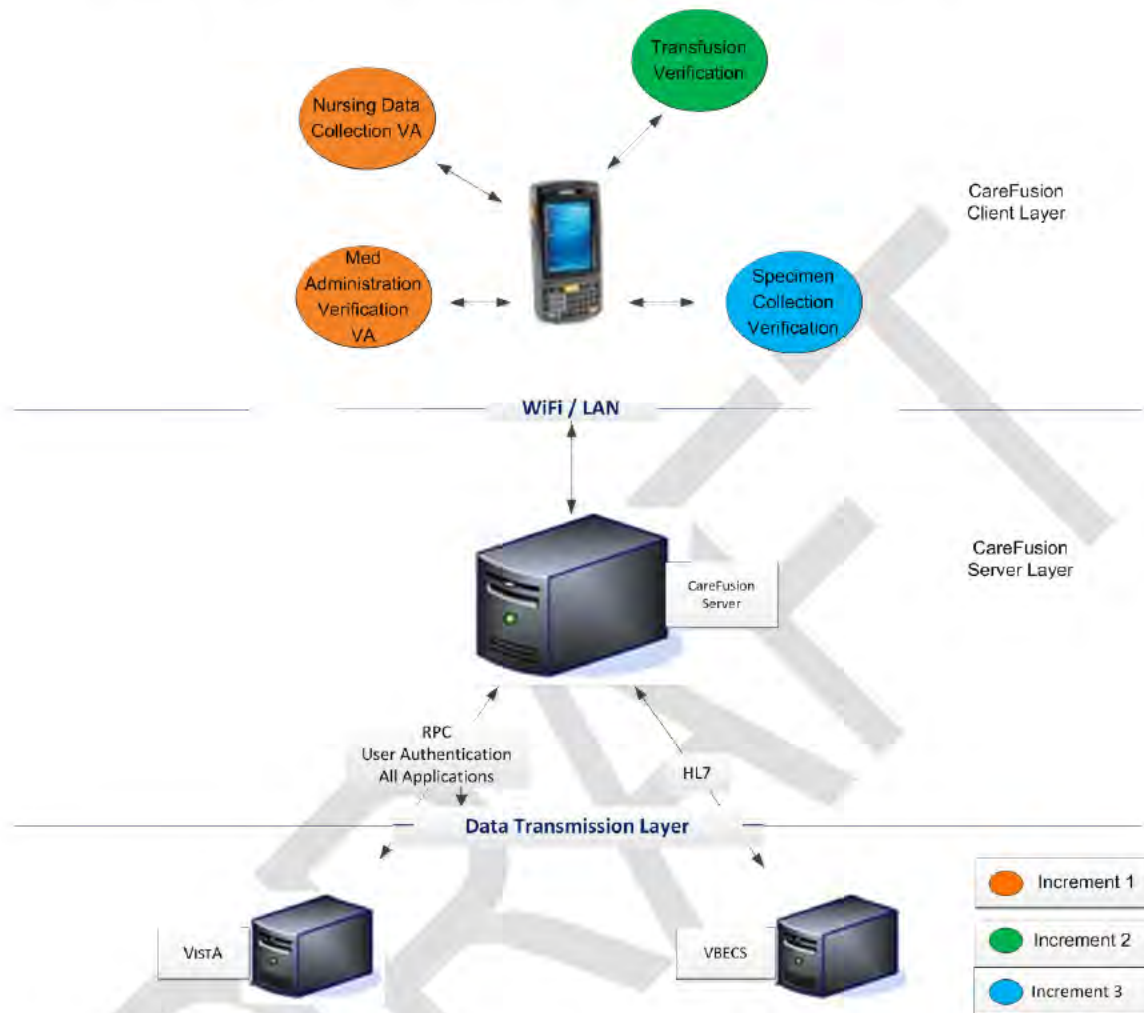
As mentioned earlier, BCE-PPI Increment 2 will also deploy the CareFusion “Ancillary Applications” WMA and NDA. While this is not always stated explicitly or shown in every diagram, it is still the case.

2.1. Overview of the System

2.1.1. Architectural Overview of the System

Figure 1 provides an overview of the functionality to be added to VHA patient care by the BCE-PPI project as a whole. The figure shows a CF EDA or desktop application device at the top level (closest to the end user) and shows the various clinical capabilities which will be enhanced with bar code capability using the CF EDA device. The second layer shows the BCE application server which acts as the primary interface between the EDA devices and the VA systems which send and receive bar code information. The BCE server has the task of translating barcode data into the HL7 messages and RPC calls used to transfer clinical information (e.g blood product orders, transfusion administration complete messages and admission/discharge/transfer data) to the VA systems involved in the Transfusion Verification system, namely VBECS, ADT, and Vista.

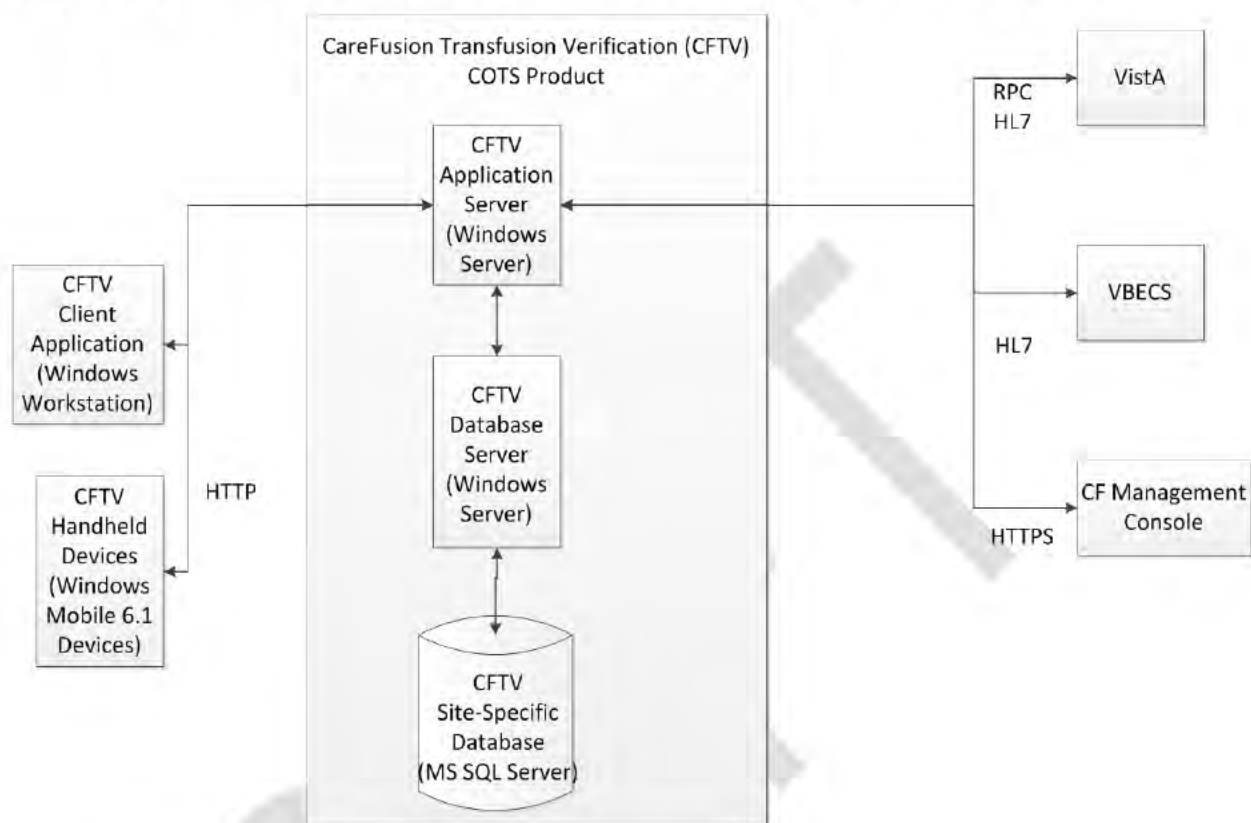
Figure 1: BCE-PPI CF Patient Point of Care (PPOC) End State Overview



Increment 2 of the BCE-PPI project will provide positive patient identification at the point of care for TV by installing a COTS TV product and interfacing it with the VBECS and other VistA applications.

Figure 2 is a high-level conceptual diagram of the BAPOC System to be delivered by increment 2:

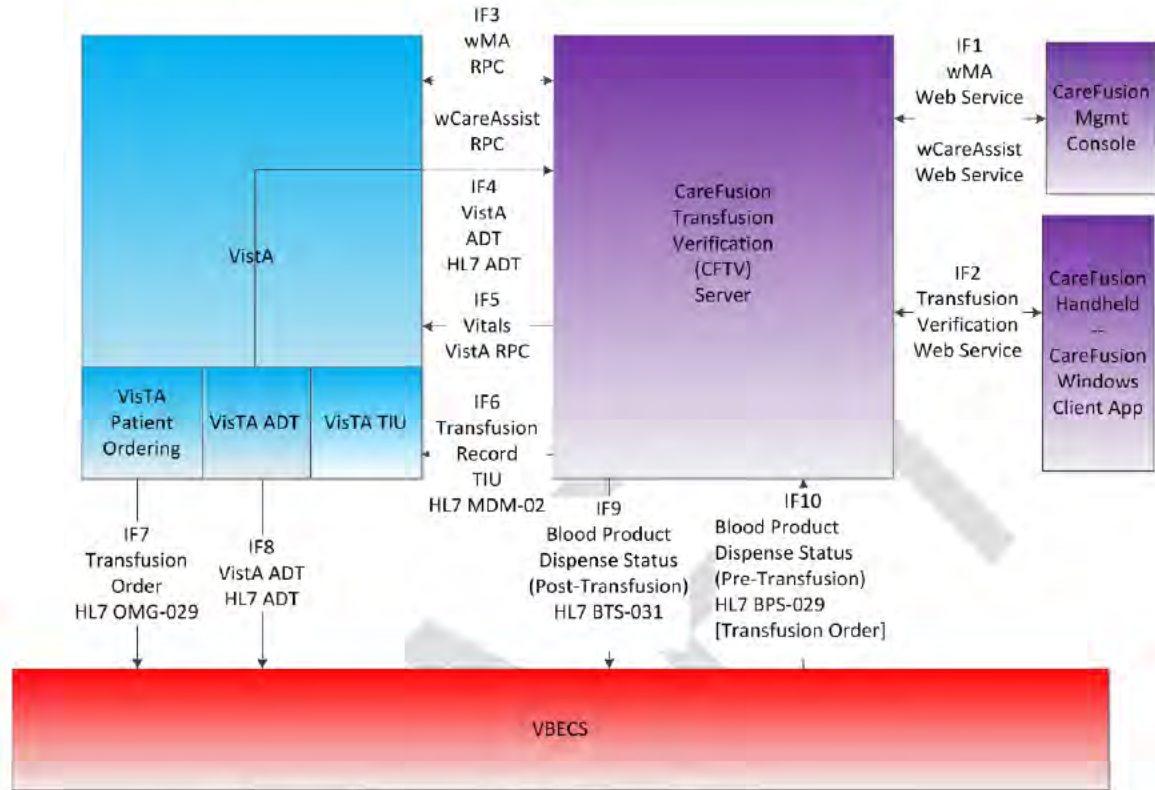
Figure 2: High-Level Conceptual Diagram of the BCE-PPI Increment 2 BAPOC System



In the figure, the CFTV EDA devices and CFTV client applications perform the task of reading bar code data from patient wristbands and blood product packaging. The bar code information is passed to the CFTV application server, where it is compared against information received from VBECS and VistA. If the information matches, the transfusion is allowed to proceed and completion information is passed from the CFTV application server to VBECS and VistA. If the information does not match, the clinician is warned and corrective measures must be taken.

An overview of the BAPOC architecture which will be implemented using the CareFusion COTS products *during increment 2* is shown in the BCE-PPI Increment II TV High-Level Communication Architecture in figure 3 which is important because it lists most of the HL7 message types that are used to connect the three kinds of servers (*VistA*, *BCE* and *VBECS*) in the overall system of systems. The legend is also important because it provides a high-level understanding of the way data flows through the system to provide fine-grained control over blood product administration using bar code data.

Figure 3: BCE-PPI Increment II TV High-Level Communication Architecture



The HL7 message types used to implement the interfaces between VistA, VBECS and CFT shown in the above figure are listed here for convenience. The detailed format for the CFTV to VBECS HL7 messages is presented in the appendices to the BCE-PPI Increment 2 Interface Control Document.

- ADT – Admission/Discharge/Transfer message
- MDM-02 – Transfusion Record Form contents (for TIU note)
- BPS-029 – Transfusion Order
- BTS-031 – Transfusion Status Update

Details on the HL7 messages used, the VistA RPC interfaces and the HL7 implementation are provided in section 7.

2.1.2. Deployment Overview

Fielding the overall system depicted in the figure above will include the following work streams:

1. VBECS and VBECS Interface patch planning, development, testing, release and deployment.
2. VistA and VistA interface patch planning, development, testing, release and deployment
3. COTS product planning, development, testing, release, and deployment.
4. Integration planning, testing, release and deployment

As noted, the COTS product to be used is the Pyxis® Transfusion Verification System supplied by CareFusion. This product:

- Ensures the blood product assigned to the patient through VBECS matches to the patient at the point of care.
- Automates the creation of the HL7 Blood Transfusion Record Form (BTRF).
- Interfaces with the VBECS Blood Bank Module.
- Documents second verifier, intravenous fluid, tubing, vital signs, and transfusion activities.
- Is intended to replace scanning into the VistA Surgery Package.

2.2. Overview of the Business Process

Figure 4 shows how the BCE PPI increment 2 project integrates blood transfusion administration and provides improved patient-centric care.

Figure 4: Overview of the Business Process for Blood Administration



In the figure, the intersecting shapes along the axes represent the primary areas involved with the use of blood products within hospital environments: laboratory, OR, POC and Nursing. These axes represent the origin, delivery, and administration of the blood products. The fact that the shapes intersect at the circle symbolizing the patient indicates that a BAPOC system must be patient-centric and that all of the elements of the system must work together to ensure patient safety and improve the quality of patient care.

Figure 5 depicts the basic workflow for a transfusion as it will be standardized as part of the BCE-PPI project. This workflow does not include alternate scenarios, such as rapid infusion or situations where a transfusion might be stopped and started, to name but a few.

In order for the transfusionist to positively identify a patient, the clinician must ask the patient for their full name and a second identifier (i.e., Date of Birth (DOB) or address). Once the clinician obtains this information, they proceed to scan the patient's wristband to verify this information.

Figure 5: Basic transfusion workflow (to be standardized by BCE-PPI Increment 2)



2.3. Business Benefits

The main business benefit resulting from this increment will be elimination of transfusion errors related to patient misidentification. Error reductions are most likely to be obtained by a systems approach that reduces reliance on human data entry and human double-checking through increased use of computer technology. Replacing human matching operations with barcode reads has the potential to substantially increase the patient to blood product matching accuracy rate.

2.4. Assumptions and Constraints

In the following sections we will describe some assumptions and constraints that impact the design and implementation of the system. Note that most of the assumptions and constraints either have been imposed by the COTS vendor or constrain the behavior of the COTS vendor in supporting the CFTV Software.

2.4.1. Design Assumptions

It is assumed that each site where the COTS EDA device will be used will have to be configured to point to the site specific server system. Configuration of the EDA systems is assumed to be the responsibility of the vendor as per the procurement contract.

Installation and configuration of the BCE server systems at the Data Center Operations (DCO) datacenters is complex and the vendor has already advised the Integrated Product Team (IPT) that the DCO infrastructure for a given site must be stood up prior to the vendors showing up for go-live activities. We have incorporated site installation by vendor teams into our deployment guide and our overall schedule. With that said, PD has worked extensively with the vendor to produce a set of installation guides which will assist DCO personnel in installing BCE servers. There is currently a CFTV Installation Guide for a full installation, meaning an installation onto a clean Windows 2008 R2 server using distribution/installation media supplied by the vendor. There is also a Technical Manual for the Vista side of the BAPOC system and an Installation Guide for the Vista patches required to make Vista and VBECS Interoperate with the CFTV COTS software. Live links to all of these documents appear in Appendix D.

It is assumed that support for the full BAPOC system will be provided using the support structure described in full in the Product Operations Manual (POM). This applies to all of the components of the BAPOC system: Vista, VBECS, ADT, the BCE server software and the BCE client software. In brief overview, end users experiencing issues with the CareFusion EDA's or desktop clients will report the problem to local IT/local support. Local support will contact NSD to obtain a local support Remedy ticket and then perform triage. Local support will involve regional support, DCO and NCO as required. If local support cannot close the ticket the issue will be escalated to National Product Support. At that point a new National Remedy ticket will be created and assigned to an HPS CLIN4 Product Specialist. The Product Specialist will own the ticket until the problem is resolved.

2.4.2. Design Constraints

2.4.2.1. Constraints Expressed as Business Rules

The bar codes that are expected to be scanned while using the TV application include;

- patient identifier on a wristband, recommended to be Code 128
- Blood product-related bar codes on the unit(s) to be transfused, ISBT Code 128 and/ or Codabar label types.

2.4.2.2. Constraints Expresses as System Specifications

- The Pyxis® TV product EDA device (MC75A) is dependent upon Wireless Infrastructure Replacement (WIR) completion.
- The Pyxis® TV product desktop application must be able to function from a wired or wireless workstation if the MC75A is unavailable. Note that this is a separate product which must be installed on a Windows workstation.
- The Pyxis® TV product must meet 100% of the documented requirements for each increment release.
- The project is dependent upon the availability of VA Technical Resources. This may impact project schedule, scope and budget.
- The Pyxis® TV product interfaces must be developed as part of a quality system as defined by Part 820 of the CFR, Quality System Regulation. This stipulation applies to vendor software development.
- All functionality in the Pyxis® TV product software shall be fully compliant with the following:
 - The American Association of Blood Banks (AABB) Standards or Blood Banks and Transfusion Services, current edition.
 - The College of American Pathologists (CAP) Laboratory Accreditation Program checklists current edition.
 - The Joint Commission (TJC), current standard edition.
 - The Food and Drug Administration (FDA).

2.4.2.3. VistA Constraints

The BCE-PPI Blood Administration – Increment 2 project will interact with the existing VistA system and that interaction imposes many constraints: VistA will feed ADT HL7 information to the CF COTS solution in an “as is” basis. No modification can occur to these ADT message streams. In other words, the ADT HL7 messaging module of VistA cannot be modified due to critical nature of that software package.

The VBECS – CF COTS solution messaging interface specifications have been agreed upon between the COTS, VistA, VBECS and BCE PPI project development teams. Any modification to this interface, specifically on the VBECS system will impact the project schedule adversely.

2.4.2.4. CareFusion Constraints

The CareFusion Pyxis TV solution relies on the existing VistA RPC call architecture to provide Vital Sign input and User authentication functionality for the TV application. The RPC's are also used with the Inpatient Pharmacy application, Wireless Medication Administration (WMA). Any changes to either the VistA side or the COTS side of the RPC COTS-VISTA interface (especially those which requiring code modifications to VistA RPC API modules).

2.5. Overview of the Significant Requirements

2.5.1. Significant Interfacing Requirements

The requirement ID numbers trace back to the RSD for the increment, which has the following file name and title:

- **File Name:** BCE-PPI_TV_RSD
- **Document Title:** The BCE-PPI Increment 2 VistA Applications / VBECS Interfacing with a COTS BAPOC System Version 1.0 RSD.

Tables 3 and 4 give a summary of the functional requirements from the RSD as reviewed and approved by the BCE-PPI Increment 2 team.

NOTE: Vitals and VBECS interfacing requirements are addressed in the second table.

Table 3: VA system's overall specifications as they pertain to the interface with BAPOC COTS application

Need #	Need	Feature #	Feature
242	Customer needs the VA System to communicate with the BAPOC system to record the details of a transfusion episode	OWNR 436.0	Send Requested Data to the BAPOC system
		OWNR 419.0	Receive Vitals Change Data from BAPOC system
		OWNR 421.0	Receive Vital Signs Data from the BAPOC system
		OWNR 422.0	Receive Data Confirmations
		OWNR 435.0	Receive Data requests from the BAPOC system

Table 4: Detailed Interface Requirements

ID	Specific Requirement / Synopsis	Requirement
Sections: 2.6.2.1 through 2.6.2.17	Vital Signs	<ul style="list-style-type: none"> Send patient's vital signs to the VistA Vitals package via existing VistA Vitals RPC to include the following: <ul style="list-style-type: none"> Blood pressure Pulse Respiration Height Weight Store the data elements above and create a unique record in the GMRV VITAL MEASUREMENT file (#120.5) for audit trail purposes. Allow users to mark Vitals record entered as error when deleting vitals record from Pyxis® TV System. Allow users to enter replacement Vitals when entered in error.
Section: 2.6.3.1.	Text Integration Utilities (TIU) note	<ul style="list-style-type: none"> Send MDM~T02 message using the generic VistA TIU HL7 interface. Create TIU progress note documenting the events and vitals included in the Transfusion Record Form on CPRS.
Sections: 2.6.4.1. through 2.6.4.5	VistA Blood Establishment Computer Software (VBECS)	<ul style="list-style-type: none"> Send patient and blood component information via HL7 BPS~029 messaging regarding blood unit status based on the following events: <ol style="list-style-type: none"> Blood units assigned to patient Blood units issued to patient Blood units have been released from patient assignment <p>**Please refer to section 7 for details on the specific data elements to be sent in the message.</p> Process acknowledgement from the Pyxis® TV System in the form of a message for any of the following conditions: <ol style="list-style-type: none"> AA- Application acknowledgement message received successfully by the Pyxis® TV System AE- Application Exception message not successfully processed AR- Application Reject message rejected by the VBECS application Acknowledge BTS~031 sent from the Pyxis® TV System when transfusion episode is complete.

ID	Specific Requirement / Synopsis	Requirement
Sections: 2.6.5.1. Through 2.6.5.29.	Pyxis® TV System	<ul style="list-style-type: none"> • Display Nursing Units List Screen with patients that have an active transfusion order. • Require user authentication using the VistA Access/Verify pair. • Positively identify patient and blood product by matching bar code values on patient with the correct blood product. • Allow users to verify patient demographics and potential adverse reactions. • Allow user to document transfusion record electronically at the point of care. • Send transfusion record to VistA using the generic TIU HL7 interface in the form of the MDM~T02 message.
Section 2.4.6.6	VistA ADT Interface	<ul style="list-style-type: none"> • Pyxis® TV System will subscribe to the following ADT message trigger events generated in VistA when any patient information has changed: <ul style="list-style-type: none"> – ADT~A01 – ADT~A03 – ADT~A04 – ADT~A08 – ADT~A11 – ADT~A12 – ADT~A13

2.5.2. Workload and Capacity Requirements

2.5.2.1. Current State of Workload Assessment

The BCE-PPI program has a set of common sense business needs. The primary performance-related business need can be expressed by saying that bar code processing must be fast enough that it doesn't alter the way the clinicians provide care. In practice this means that there cannot be significant delays in reading a bar code, receiving transfusion orders, or in any other part of the transfusion verification process where a clinician provides care.

The common sense business need to state and understand is hard to quantify. To actually specify what is "fast enough" for a clinical system it is necessary to develop quantitative requirements, metrics and thresholds. In this section we describe what the BCE-PPI team has done to develop performance requirements that can be used for capacity planning, performance testing, etc.

The BCE-PPI Transfusion Verification Requirements Specification Document (RSD) contains no explicit performance requirements as indicated in table 5. Table 5 shows the values assumed for further performance analysis:

Table 5: Workload Requirements

Requirement ID	Requirement
No RSD ID (The RSD for BCE-PPI does not have a specific requirement for performance.)	6 transfusion transactions in 3 minutes - from the Capacity and Performance Engineering (CPE) report. This figure represents a “disaster scenario”, meaning it represents a rate which would occur after a disaster in the vicinity of the hospital. Most hospitals do far fewer transactions than this under normal conditions.

Based on these performance requirements the SDE members of the BCE-PPI team sized VM’s for use at test sites. The initial values for RAM, CPU, network and disk capacities for the test site VM’s came from CareFusion. The values were based on their experience with sizing a physical server to meet the transactional workload requirements for a single hospital.

Once the initial values for the VM configuration were in hand, capacity planning was done using the results of a load test performed in Dallas by the Capacity and Performance Engineering group within SDE. The test was performed using the Dallas test servers as configured in the field. The servers were monitored while 3 users performed test transfusions for a period of thirty minutes and the performance of the servers was measured using CPE’s standard monitoring software.

The workload used for the initial capacity plan was generated by having 3 users perform as many transactions as they could for a period of 30 minutes. The report summarizes creation of the workload as follows:

The following data outlines the test details and the workload created on the System Under Test (SUT):

- The Transfusion test workload exceeded a typical daily workload
 - Workload intensity: 6 transfusion transactions every 3 minutes.
 - Large disaster/catastrophe scenario
 - A typical daily load would be 1-2 transfusion patients processed per day.
- Number of manual testers: 3
- Total throughput of test:
 - 12 patients processed
 - 114 records/transaction processed

The steps in a transaction which each user followed are summarized in the report. As the report notes, the transaction workload created in this fashion far exceeds the number of transfusions that would be processed on a typical day.

The CPE report presents the results of this manual test. It concludes that the BCE database server and BCE database server can as configured in Dallas can support the transaction rates required for the high availability scenario (i.e. the disaster scenario).

The CPE report is embedded here for convenience.



BCE_Capacity_Analysis
Report_v1 1.docx

2.5.2.2. Initial Capacity Plan

The physical design of the system presented above and the VM configuration in the contract with DCO (the 2013 and 2014 SLAMs) are based on the results of the CPE report. This applies mostly to the database servers as the number of BCE application servers is determined by geography—usually there is one BCE application server per VistA site. (The case of satellites, where several sites share a BCE server is an exception.)

In reality, the physical system design presented in section 2.3 is the initial capacity plan, and VM's will be deployed during rollout according that design.

2.5.2.3. Capacity Planning Concerns

In essence, the capacity planning done to this point uses the results measured for 3 users doing transfusions for 12 patients for 30 minutes. It is certainly legitimate to wonder if these results can safely be extrapolated to the more than 1000 Pyxis TV users who will be able to perform thousands of transactions per hour. It is also perfectly legitimate to wonder if the results obtained on a single system can be scaled out to the total VA deployment of more than 140 BCE App servers. Finally, it is perfectly legitimate to point out that the results obtained for a single server do not consider Wide Area Network latency, delays from security processing at network boundaries and other performance issues related to networking.

When the above considerations are combined and weighed, it becomes clear that the true capacity of the CF Pyxis TV application when scaled out to the full VA enterprise is currently unknown.

As previously mentioned, these concerns are not unique to the CareFusion applications. It is often difficult to create an accurate model of the load on an application at scale. It is very difficult to model network latency and WAN behavior accurately. It is difficult to create a simulation environment that models reality accurately enough to improve capacity planning. Taken together, these difficulties make phased deployment with capacity adjustment the standard approach. With that said, it is crucial that the performance results for the first few sites be used to refine the initial estimates, because the initial deployment provides real data on network latency, the load real users place on the application, and the first real performance metrics for the application in production.

All of these concerns are expressed and addressed in the summary from the CPE testing lead which accompanies the CPE Capacity Analysis report for the project:

To summarize, the following recommendation was made:

Capacity analysis provides an estimate of the anticipated performance for systems and cannot account for other external factors that may adversely influence the utilization of systems deployed in production. Therefore, capacity analysis practices should be engaged in an on-going basis to further quantify the actual workload in production as a preventative measure to insure system health

The analysis indicates that the BCE application deployed on a VMware platform, as staged in the test environment, is adequate to support a single site workload. The End-User response time during the course of the testing was perceived as acceptable. The BCE system deployed in a virtualized guest system, as specified in the (SDE-provided) SDD, should be capable of supporting the BCE application for a single site. *It is recommended that post-deployment instrumentation be utilized to further validate the sizing and calibrate the capacity model for the BCE application, help plan subsequent migrations, and help configure the VM guests.*

We look forward to engaging in the next steps of BCE Project.

(The italics in the above citation were added during preparation of this document.)

2.5.3. Operational Requirements

There are no operational requirements per se associated with BCE-PPI Transfusion Verification in the existing RSD or in ReqPro. However, The term “operational requirements” requires some interpretation. In this section of the SDD, we have restricted functional requirements (as tabulated in the preceding section) to be those related to how the system functions in relation to other systems. In essence these are integration requirements. We will use operational requirements to mean the way the system looks to people (users and managers) as opposed to the way it looks to other systems. With this distinction in mind, many of the functional requirements from the RSD can be viewed as operational requirements.

Table 6 shows the Operational Requirements for BCE increment 2.

Table 6: Operational Requirements

Functional Requirement ID	Requirement
25	The Pyxis® Transfusion Verification system shall display a screen called the Nursing Units List screen with patients that have active transfusion orders when login is successful. NOTE: Facility specific configuration determines the number of hours, patients and the corresponding orders display.
26	The Pyxis® Transfusion Verification system shall display the following message if login is unsuccessful: Incorrect User ID/Password – Please re-enter
27	The Pyxis® Transfusion Verification system shall allow one or more units in the Nursing Units List screen to be selected and then select patients to access a list of patients. NOTE: The patient location, priority (stat (*) or routine (R)) and patient name

Functional Requirement ID	Requirement
	display for review.
28	The Pyxis® Transfusion Verification system shall allow the user to scan the patient's wristband or enter the patient identifier.
29	<p>The Pyxis® Transfusion Verification system shall allow the user to initially confirm the patient by displaying the following and asking if this is the correct patient:</p> <ul style="list-style-type: none"> • Patient's name • Patient's ID or Alternate ID • Location • DOB • Sex • Age • Race • Provider
30	<p>The Pyxis® Transfusion Verification system shall allow manual entry of patient's record per local configuration settings.</p> <p>NOTE: The user must enter the reason for manual entry as required per local configuration settings. This comment is transmitted as part of the post transfusion message.</p>
31	<p>The Pyxis® Transfusion Verification system shall allow the user to additionally confirm the following:</p> <p>Patient Demographics</p> <p>Allergy Confirmation or any potential adverse drug reaction</p>
32	<p>The Pyxis® Transfusion Verification system shall scan the blood unit to start the transfusion process.</p> <p>NOTE: This is an optional configuration at the Facility and shall display a message if it is the user's first time accessing the orders screen.</p>
33	The Pyxis® Transfusion Verification system shall display notifications throughout the transfusion process.
34	The Pyxis® Transfusion Verification system shall provide the user with several menus that provide additional patient related information.
35	<p>The Pyxis® Transfusion Verification system shall have the ability to do the following:</p> <p>Refresh orders through the Refresh Order List</p> <p>Obtain a unit history report</p> <p>Enter Patient Vitals</p>
36	<p>The Pyxis® Transfusion Verification system shall allow entering blood product ID manually per local configuration settings.</p> <p>NOTE: The user must enter the reason for manual entry as required per local configuration settings. This comment is transmitted as part of the post transfusion message.</p>
37	<p>The Pyxis® Transfusion Verification system shall display the following from the orders screen:</p> <p>Screen name</p> <p>User identification number</p>

Functional Requirement ID	Requirement
	Patient name and Identification number Blood type Blood bank number Order List Status Type Selection
38	The Pyxis® Transfusion Verification system shall allow the following when viewing Transfusion Activities: Unit ID Order Number (N/A in VA settings) Status Priority Donor Blood Type Product Product Code Transfusion Requirements Issue Time Expiration Date Ordering Provider Antibody Screen Crossmatch Compatibilities Transfusing Time Stop Time Stop Reason Stop
39	The Pyxis® Transfusion Verification system shall allow the blood unit with active orders to be transfused. The following information is scanned: Production Date Time Barcode Unit ID Barcode Product Code Barcode ABO/Rh Barcode Collection Date/Time Barcode Expiration Date/Time Barcode Special Testing Barcode
40	The Pyxis® Transfusion Verification system shall allow the user the select the transfusion.
41	The Pyxis® Transfusion Verification system shall display an error message when any of the scanned information does not match any transfusion on the list.
42	The Pyxis® Transfusion Verification system shall allow a second scan for the user to scan the Unit ID bar code on the blood tag/label and compare it against the Unit ID barcode that is imprinted on the unit bag itself.
43	The Pyxis® Transfusion Verification system shall allow the facility to configure an allowable time frame for the transfusion of an issued blood product.
44	The Pyxis® Transfusion Verification system shall allow the following which are optional entries: Infusion Device and Number Admin Set and Filter Entry option

Functional Requirement ID	Requirement
	Lot Number Indication for Transfusion drop-down Entry for Primary Blood Bank Number Enter Vital Signs Warning Message for a Suspected Transfusion Reaction Pre-Transfusion Checklist Witness Verification Transfusion Begin Time Capture, if system not configured for Match Confirmation NOTE: This are configurable entries at the Facility.
45	The Pyxis® Transfusion Verification system shall allow the user to enter the stopped transfusion. Enter Vital Signs for Stopped Transfusion Record Volume Infused For Stopped Transfusion NOTE: The Stop Action drop-down list is populated by the Facility through the Pyxis Point of Verification console.
46	The Pyxis® Transfusion Verification system shall allow the user to continue to transfuse stopped blood unit.
47	The Pyxis® Transfusion Verification system shall allow the user to document the volume infused.
48	The Pyxis® Transfusion Verification system shall allow documenting exceeding the maximum time transfused.
49	The Pyxis® Transfusion Verification system shall allow a user to edit a transfusion record in normal flow.
50	The Pyxis® Transfusion Verification system shall allow working with Rapid Infusion. NOTE: Rapid infusion is designed to provide a more flexible workflow for use in the Operating Room (OR) and emergent environments.
51	The Pyxis® Transfusion Verification system shall subscribe to VISTA ADT for patient updates.
52	The Pyxis® Transfusion Verification system shall recognize the different divisions in a multi-divisional medical center.

2.5.4. Overview of the Technical Requirements

Technical Requirements usually refer to things like accounting for time zone differences, ensuring a self-consistent Graphical User Interface (GUI), etc. They are usually detailed in the RSD. However, the version of the RSD used in the preparation of this document does not have a section on Technical requirements. With that said, if we define “technical requirements” to be those related to multidivisional behavior, performance, reliability and security then the technical requirements for the BAPOC system from the RSD are as follows:

2.5.4.1. Multi-Divisional Specifications

The BCE-PPI Blood Administration/Pyxis® Transfusion Verification system shall allow data to be captured, reported, and shared at the division and consolidated VistA as configured. (VBECS patient testing and blood availability information and records are division specific).

2.5.4.2. Performance Specifications

The requirements state in this section refer to availability, usability and sustainability. They do not refer to performance in the sense of responsiveness under load. Those requirements have been discussed previously, in section 2.5.2

1. The BCE-PPI Blood Administration/Pyxis® Transfusion Verification system shall be free of any major defects that will render the system disabled or non-functional.
2. The BCE-PPI Blood Administration/Pyxis® Transfusion Verification system shall operate on various devices; is not restricted to how the platform is identified, are upgradeable and sustained overtime.
3. The BCE-PPI Blood Administration/Pyxis® Transfusion Verification system shall provide opportunities to reduce the total number of SOLUTION instances needed to support all medical centers, provides any requirements for proximity to end users, and describe tools included for remote management of the system.

2.5.4.3. Quality Attributes Specifications

All functionality shall be compliant with existing blood bank standards, standards of accrediting agencies, FDA regulations and VA policies.

2.5.4.4. Reliability Specifications

When data is entered or updated from the BAPOC system, there shall be an acknowledgement from the VBECS system of receipt of that data.

2.5.4.5. Usability Specifications

In regard to the COTS Blood Administration Point of Care (BAPOC) System, VA has requested documentation from the vendor concerning previous work performed pertaining to use error/usability (such as, but not limited to, the vendor's 510K submission, usability data, use error risk analysis and mitigation responses, etc). VHA will review the information provided to determine the need for risk mitigation plans, i.e., VHA operating procedures, implementation and maintenance processes, training.

2.5.5. Overview of the Security and Privacy Requirements

The high-level security requirements from the RSD are as follows:

1. The BCE-PPI Blood Administration/Pyxis® Transfusion Verification system shall provide role-based security to restrict access to information as established for the user in the VISTA system.

2. The BCE-PPI Blood Administration/Pyxis® Transfusion Verification system provides secure authentication to the VISTA system.
3. The BCE-PPI Blood Administration/Pyxis® Transfusion Verification system shall describe tools provided with the SOLUTION to enable VA to fully manage VA patient and security data stored within the SOLUTION.

For purposes of software development and design these have been decomposed into the detailed requirements listed in table 7:

Table 7: Security Requirements

ID	Requirement
Section 2.13	<ul style="list-style-type: none"> • Use VistA Security keys from the VistA CF package (namespace: MJCF) to lock down Pyxis® TV options based on the following user access roles: <ol style="list-style-type: none"> 1. MJCF TV Administrator – This Administrator key allows the user to access the Pyxis® TV application and both the Configuration and Reports portlets on the CFMC (Configuration Manager). 2. MJCF TV Reports – This Reports key allows the user to access the Pyxis® TV application and the Reports portlet on the Configuration Manager. 3. MJCF TV User – This User key allows the user to access the Pyxis® TV application. • Restrict access with the Pyxis® TV for the following functionality: <ol style="list-style-type: none"> 1. Access to Pyxis® TV application. 2. Ability to witness a transfusion. 3. Set/Change Device Location (needed for rapid transfusion). 4. Edit All Entries.

An explanation of how these access control requirements are met using VistA Access and Verify codes for authentication and VistA menus, menu options and keys for authorization appears later in this section.

User security will follow existing policies for user access. Users will gain access to the user interfaces of the CF TV system by authenticating against VistA. The user interfaces which have controlled access are the CareFusion Management Console (CFMC), the handheld CFTV client (EDA) and the CFTV desktop client.

VistA authentication will be used to provide accurate identification of staff by validating the currently established security keys and contexts at the user and facility level. The Product Operations Manual provides an in-depth discussion of how CareFusion TV uses the VistA Access Code and Verify code to authenticate a user and to control a user's access to CareFusion TV functionality via the CareFusion Management Console (CFMC) web client application. A summary is provided here for convenience.

A specific user's roles are determined by the user's assigned VistA menus and keys which have been granted by the local VistA support. Table 8 specifies how user authorization and authentication roles for

both the Transfusion Verification Client application and CareFusion Management Console web client application are aligned with VistA menus, options, and keys for the CFTV clients.

Table 8: User Authorization and Authentication roles

CFTV User Interface	
<u>Transfusion Verification Client Applications</u> (Desktop and PDA's)	<p>User Authentication – User VISTA access/verify code</p> <p>User Authorization – User must be assigned VISTA MJCF TV USER key and MJCF TV USER secondary menu</p>
<u>CareFusion Management Console Web Client</u> (Internet Explorer)	<p>User Authentication – User VISTA access/verify code</p> <p>User Authorization – Role-based access control by the VISTA secondary menus assigned to a particular user.</p> <p>NOTE: Although User Authentication functions similarly for both clients and CFMC, user authorization for the CareFusion Management Console web client application is more complex due to the number of roles and resources restricted by the RBAC policy.</p> <p>See the next table for CFMC user role definitions and the mapping of these roles to VistA menus, options and keys.</p>

To meet the above requirements, role-based security will be provided for the BAPOC system, meaning that user access to information will be contingent upon their VA-defined role based permissions.

Table 9: CareFusion Pyxis TV Security Roles and Corresponding VistA Access

USER ROLE	Transfuses	VISTA Menus Option	VISTA Security Keys	Client Application Access	CareFusion Management Console Access
RN	Yes	MJCF TV USER	MJCF TV USER	Yes	N/A
Nurse Manager	Yes	MJCF TV USER MJCF TV REPORTS	MJCF TV USER	Yes	Transfusion Verification Admin Report Transfusion Verification Reports

USER ROLE	Transfuses	VISTA Menus Option	VISTA Security Keys	Client Application Access	CareFusion Management Console Access
Nurse Manager	No	MJCF TV REPORTS	N/A	No	Transfusion Verification Admin Report Transfusion Verification Report
BCE Coordinator	Yes	MJCF TV USER MJCF TV ADMINISTRATOR	MJCF TV USER	Yes	Transfusion Verification Admin Report Transfusion Verification Reports Transfusion Verification Configuration
BCE Coordinator	No	MJCF TV ADMINISTRATOR	N/A	No	Transfusion Verification Admin Report Transfusion Verification Reports Transfusion Verification Configuration
System Administrator	NO	MJCF TV APP ADMIN	N/A	No	Access to all Portlets on CFMC

The CF Pyxis TV solution will not store data on the EDAs.

2.5.5.1. Wireless Security

The CF Pyxis® Point of Care applications have been designed to fully comply with the VA's FIPS 140-2 encryption requirements.

2.5.6. System Criticality and High Availability Requirements

The following system criticality and high availability (HA) requirements apply to BCE PPI increment 2:

- The BCE-PPI Increment 2 – Blood Administration software shall have 99.7-percent availability. A caveat to this statement is when a facility's computer system is down manual recording of transfusion information will be permitted.

- There shall be vendor customer service provided 24 hours a day and 365 days a year.
- The VA is required to activate their existing contingency plan(s) to revert back to their manual or pre-existing failover processes in the event a COTS application failure occurs.

The redundant hardware and the failover procedures to be used in meeting the HA for BCE PPI increment 2 are described later in this document, in section 3.3.1. Design responsibility for meeting HA requirements falls on the SDE members of the core team and on the DCO staff.

In the Information System Contingency Plan (ISCP) created by DCO establishes procedures to recover AITC's **Bar Code Expansion – Positive Patient Identification (BCE)** following a disruption. That document specifies that **BCE** is designated as Mission Critical for disaster recovery. The recovery time objective (RTO) for this level of support is that it will be operational within 12 hours after a disaster declaration. Backup is to replicated DASD at a remote site with a secondary backup to tape media. The recovery point objective (RPO) is production data loss of no more than 2 hours.

2.5.7. Special Device Requirements

The vendor recommends the Motorola® MC75AO because of its scanning capability, portability, and hardware-level wireless security compliance to FIPS 140-2 policy, in accordance with VA wireless security policy. The named Motorola device has undergone bar code scan engine testing and approval by the Bar Code Resource Office (BCRO) per VHA Directive 2006-069.

General EDA capabilities are:

- Ruggedized device
- Windows Mobile 6.1 Operating System (or later)
- Extended Battery
- Tethered Stylus
- Charging Station
- 1D and 2D Bar Code Scanning
- 802.11b/g radio Wi-Fi Protected Access/Wired Equivalent Privacy (WPA/WEP/WPA2-802.11i)
- FIPS 140-2 encryption certified for wireless security.
- Healthcare Plastics Housing

3. Conceptual Design

3.1. Conceptual Application Design

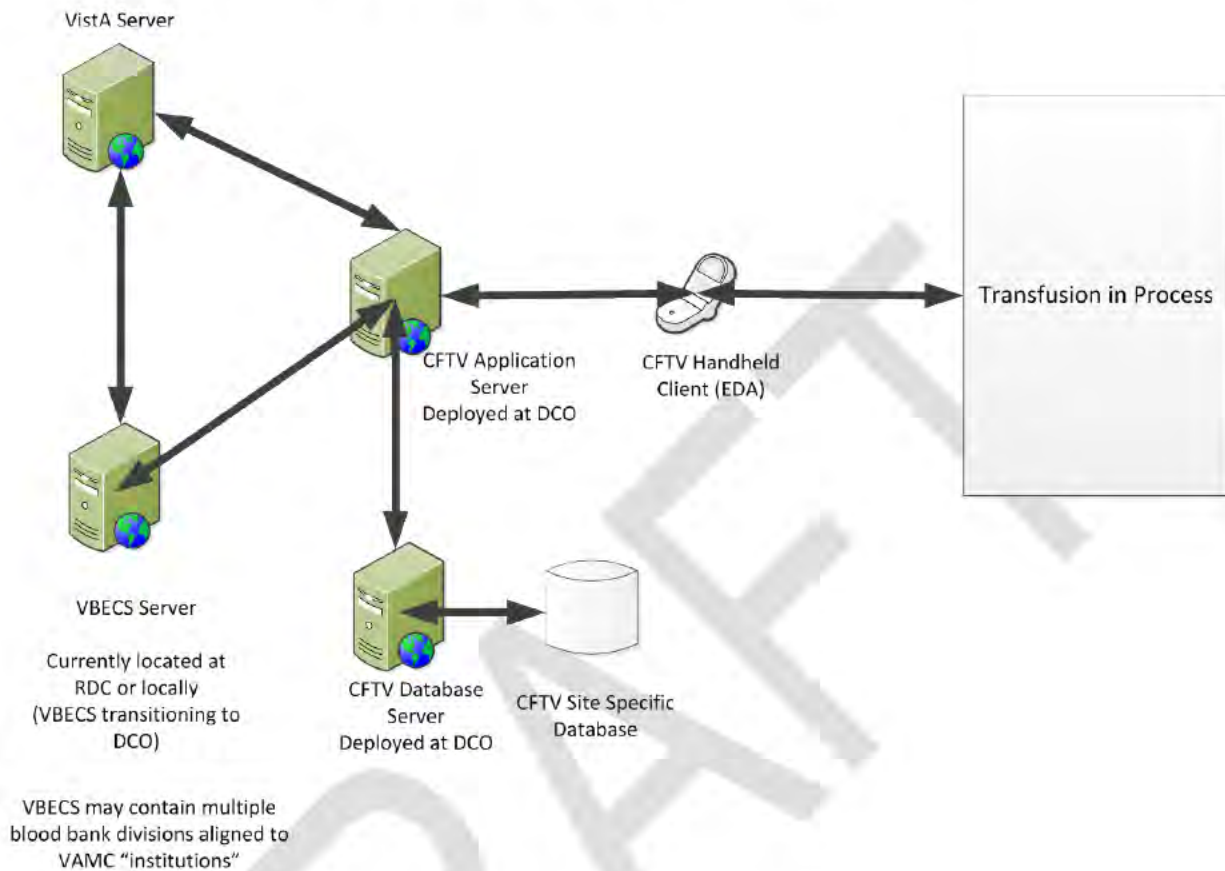
The subsections below will further elaborate the Conceptual Application Design for BCE-PPI Transfusion Verification.

3.1.1. Application Context

The CareFusion Pyxis® TV system will allow users to positively identify patients at the point of care by matching patients with the blood products to be infused. In order to accomplish this, the overall system will integrate VistA components, VBECS and the CF Pyxis® TV applications into a complete system architecture which meets the requirements presented in the previous section.

Figure 6 gives a very high-level view of the overall system architecture. (Note that laptops and desktop clients are not shown). The key architectural facts displayed by the diagram are that both the VBECS and VistA servers may be deployed either at a DCO datacenter, an RDC or locally. In practice the VistA servers are generally deployed at RDC's. In the past, VBECS servers have been deployed locally, but at present most VBECS servers are hosted on VM's in the RDC's. (VBECS is transitioning to DCO later this year.) In either case the fact that either the VistA Server or the VBECS server can be physically located in a different time zone than the BCE server hosting the CF software must be accounted for in the deployment design. In addition, the time zone of both the BCE server software and the CFTV client software must be considered. If necessary, duplicate BCE servers will be stood up and configured to be in the same time zone as their VBECS and VistA partners.

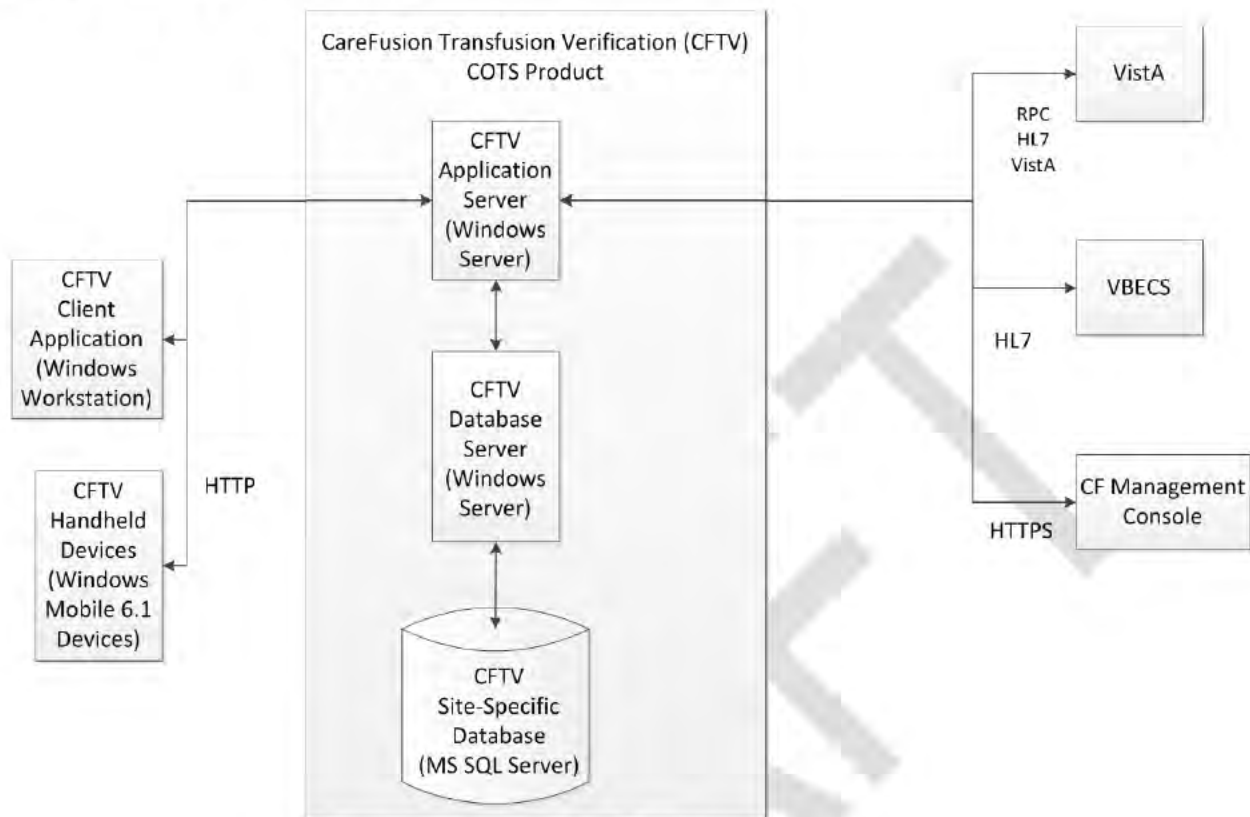
Figure 6: High-level Overview of Bar Code Enabled Transfusion Verification



At the 50,000 foot level, there are four kinds of data exchanges in the overall BAPOC system to be provided by the increment:

1. Transfusion information flows constantly between VBECs and the Pyxis Transfusion Verification Application (also known as Pyxis TV) in the form of HL7 messages.
2. ADT information flows Between VistA and VBECs. It also flows between VistA and the Pyxis TV application.
3. Vital Sign data flows from the Pyxis TV application to VistA.
4. The Pyxis TV sends the information required to formulate a TV progress note to the VistA system.

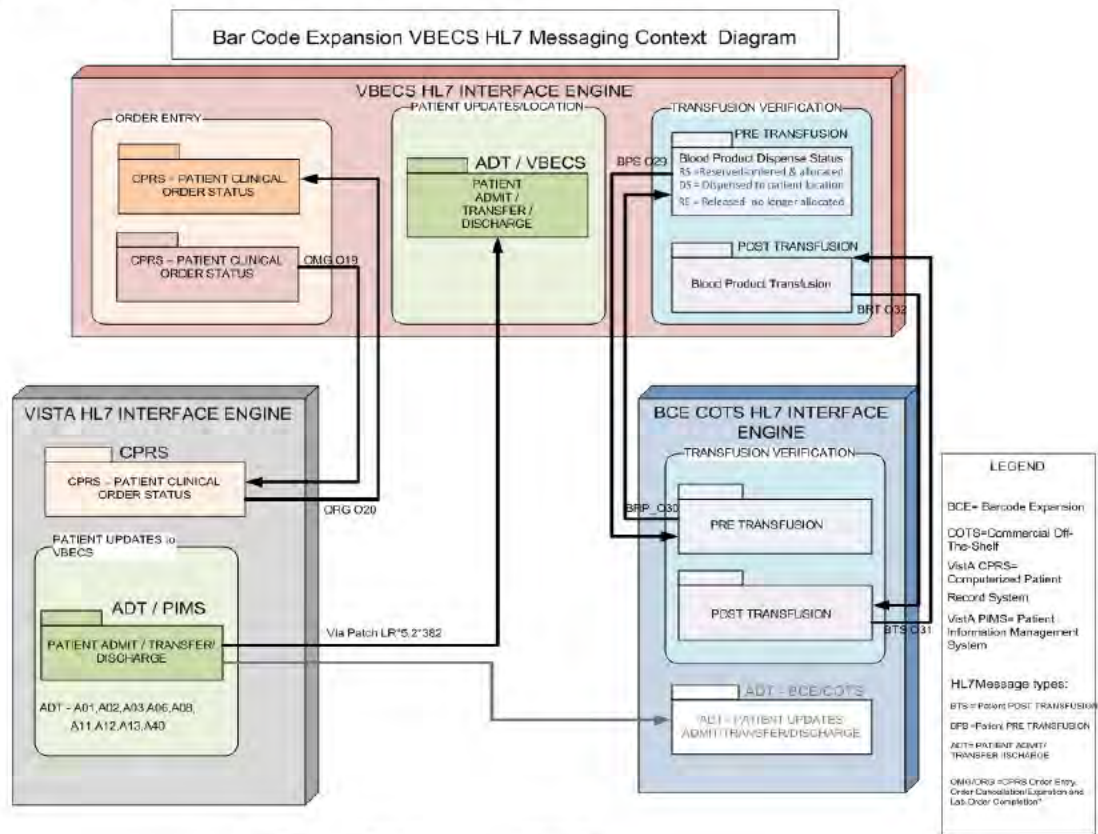
Figure 7: High-level architecture



For transfusion-related information, communication between the BCE server and the VBECS and VistA servers is carried out using HL7 messages. The exact nature of the messages and the VistA and VBECS subsystems which receive HL7 messages they receive are spelled out later in this document, mainly in section 7.

The next figure begins the task of spelling out how the HL7 interface between VBECS, VistA and the CFTV server's works. The figure is a message context diagram for BCE-PPI increment 2, showing how the various VistA, VBECS and CFTV components interact by exchanging HL7 messages. The arrows in the figure represent the key system interfaces; they are labeled with the HL7 message which is used to implement the interface. The HL7 messages used to create the TIU note are not shown in the figure, however, they will be explained later in this document.

Figure 8: BCE PPI TV Message Context Diagram



3.1.2. Application Locations

Table 10: Application Locations

Application Component	Description	Location at Which Component is Run	Type
Pyxis® Med Admin VA bapiservice	Web service application that enables communication between Pyxis® Med Admin VA and VistA Vitals package via RPC architecture. Specific to WMA	BCE App Server installed at a DCO datacenter	Server component
Pyxis® Nurse Assist VA HHC Client application	Client GUI application that allows clinician to enter/edit patient at the point of care.	EDA/ Wireless workstation, installed at VAMC	Client GUI
wswCareAssist	Web service application that enables communication between Pyxis® Nurse Assist VA and VistA Vitals package via RPC architecture. Specific to NDC	BCE App Server DCO datacenter	Server component
Pyxis® TVVA	Client GUI application that allows user to positively identify patients and document blood product infusion encounter.	EDA/ Wireless workstation, installed at VAMC	Client GUI
WBCService	Web service application that enables communication between Pyxis® TVVA and VistA Vitals package via RPC architecture.	BCE App Server DCO datacenter	Server component
CFMC	CareFusion Management Console Allows users to manage and configure settings of the CF app server.	BCE App Server DCO datacenter	Web Client run at administrator's workstation plus web application running on the BCE app server

3.1.3. Application Users

The users for the bar code enabled BAPOC system to be fielded during increment 2 are listed in Table 11.

Table 11: Application Users

Application Component	Location	User
Blood Administration	All sites	Transfusionists who are trained in the use of the Pyxis Transfusion Verification Application.
Physicians	All sites	Physicians who read the progress note prepared by the TIU system and use the note for treatment decisions
Nurses	All sites	Nurses who enter patient identification information into the system and verify that barcode results for patient data match the manual entries they have made.

All of these user types must be considered in system design, in system testing and in system deployment. The system will be designed to required proper user authentication and authorization of all user types

3.2. Conceptual Data Design

The subsections below will elaborate the Conceptual Data Design for BCE-PPI.

3.2.1. Project Conceptual Data Model

In essence, the conceptual data model for BCE-PPI increment 2 is given by the preceding message context diagram (figure 8): the data of concern is the payloads of the HL7 messages which weave the VBECS, VistA and CFTV servers into a cohesive system of systems for transfusion verification. Obviously there is non-message data in the system, but it is stored in existing databases in standard ways. To say this differently, the way VistA and VBECS process HL7 messages is not changed by the CFTV integration and the way that data from the messages is stored in the VistA database is not changed either. . For this reason, this document does not include a description of the VBECS and VistA databases because such a description is outside of the BCE-PPI project scope. The reader is referred to appendix D where a number of key documents from the VistA Document Library are listed. The integrated system does require one new message and one new interface. The new interface is a two-way HL7 exchange of ADT messages between the VistA ADT subsystem and the BCE Application server. VistA sends ADT data to VBECS and VistA sends ADT data to the BCE Application Server. The BCE server and VBECS do not exchange ADT data. The new message is the ADT message involved in the VistA to BCE server interface.

The formats of the HL7 messages exchanged in the integrated system are briefly described in the Interface section of this document (section 7.2). Changes made to VistA and VBECS to accommodate the new ADT messages are in VistA patch LR*5.2*382. The software modifications made in the patch are described in the patch documentation and will not be described further in this document.

When HL7 messages are received by the M routine associated with the subscriber protocols. The M routine acts on the message and updates the VistA database as required. HL7 message processing is described in depth in the VistA Document Library and a wealth of information is available at the following link.

[http://\[REDACTED\]](http://[REDACTED])

The VistA Health Level Seven (HL7) Site Manager and Developer Manual is an excellent starting point. It has been recently updated and provides an overview of how the current HL7 implementation works. A PDF version of this guide is available at the following link.

[http://\[REDACTED\]](http://[REDACTED])

RPC calls are fielded by the RPC listener on VistA. The listener dispatches to the Remote Procedure being called. The Remote Procedure updates the VistA database as needed.

3.2.2. Conceptual Database Information

In principal there are three databases for each instance (site) of the integrated system: the VistA database, the VBECS database and the CareFusion Microsoft SQL database. The VBECS and VistA databases hold clinical data which is used directly for patient care. The CareFusion Microsoft SQL Database) which will refer to from now as the BCE site-specific database) holds clinical data as well blood component orders (transfusion orders, for example) but that data is only used to support the operation of the client devices, for example to display the blood component order corresponding to a blood product barcode on the EDA device.

VistA software components which interact with the software to be deployed during this project increment do not require enhancements or modifications to the existing database. This also applies to VBECS. The exception to this rule is of course the new ADT message exchange.

The CareFusion Pyxis Transfusion Verification application requires the implementation of a Microsoft SQL RDBMS to support processing by the HL7 interface engine. (Again, this is the database we are referring to as the BCE site-specific database.) The database structure and contents are proprietary intellectual property. For that reason this document will not describe the BCE site-specific database. Any issues involving the BCE site-specific database will need to be referred to the vendor for resolution. National Support Remedy tickets will need to be created in order to engage the vendor's support team.

3.3. Conceptual Infrastructure Design

The subsections below will further identify the Conceptual Infrastructure Design for BCE-PPI.

3.3.1. System Criticality and High Availability

The BCE-PPI Transfusion Verification solution is vital to direct patient care and must be available at all VA medical facilities where transfusions are performed and it must be available on a 24x7 basis. For that reason the COTS solution is considered a critical system and the system design must support high availability as defined for a VA critical system. The requirements for high availability have been described in section 2.5.6. In brief, the system is required to be operational 99.7% of the time and the longest allowed outage is 12 hours after a disaster is declared.

Providing high availability for the VistA systems is the responsibility of the data centers where the Vista servers are deployed. Server Redundancy and Failover procedures for VistA are outside of the scope for this document but see the references for VistA in appendix D.

Providing high availability for the VBECS systems is the responsibility of the data centers where the VBECS servers are hosted or the local site if there is still a physical server involved. (VBCES servers are scheduled to be transitioned to VM's hosted by DCO during 2014 so physical VBECS servers will soon be a thing of the past and DCO will be responsible for VBECS high availability.) Server Redundancy and Failover Procedures for VBECS are outside the scope of this document, but see the references in for VBECs in appendix D.

To support high availability, the server-hosted components of the CareFusion Pyxis (COTS) applications will be deployed in on virtual machines (VM's) located at the AITC and PITC datacenters operated by DCO. These virtual servers will be created using VMware.

In the proposed hardware configuration each primary BCE database server is paired with an identical backup server. The primary and backup servers both have access to the production databases which are created on SAN hardware. MS SQL clustering software is used to support rapid switching between the primary and backup server in the event that the primary server hangs or goes down. The use of Microsoft SQL server failover clusters provides automatic failover.

The primary BCE application servers do not have redundant backup servers and automated failover is not provided. The BCE application servers at the DR center are not online and in the event of a primary server failure the DR center backup VM will have to be made current using a snapshot of the primary server before operation can be switched to the backup server. An alternative to using the DR center server for failover is to provision a new server at the primary data center (AITC) and then restore a snapshot. In either case manual steps will be required and there will be an outage for that BCE site until the newly provisioned server comes online as the primary server.

The table below lists the failure scenarios which the HA plan must consider.

The number of failures allowed is based on 99.7% uptime.

$365 \text{ days/yr} \times 24 \text{ hrs/day} = 8760 \text{ hours/year}$
 $8760 \text{ hours} \times 0.997 = 8733 \text{ hours required uptime/year}$
 $8760 - 8733 = 26.2 \text{ hours permitted downtime/year}$

The table assumes that the DR BCE database server is partnered in an MS SQL cluster for the BCE database.

Failure Scenario	HA methodology	Recovery Steps	Time to recover	Number of in
------------------	----------------	----------------	-----------------	--------------

				permitted for uptime
BCE App Server Failure (loss of OS on VM)	Manual restoration of VM	Provision a new VM Restore snapshot to new VM (Should already be configured to talk to site-specific database, Vista and VBECS) Do a normal startup Verify green interface lights in CFIE Resume normal operation	4 to 8 hours if snapshot available Longer if VM must be restored from a backup tape and reconfigured	3 if time to re- operations is 8 6 if time to re- hours
BCE SQL Server Failure	SQL Server Failover Cluster plus SAN replication plus offsite backup Primary VM is at AITC, secondary is at PITC SAN replication occurs between AITC and PITC	Failover to the secondary VM Resume operation immediately if the physical databases are intact. Restore physical databases from SAN replicates if they are damaged Restore physical databases from backup if SAN replicates are not available	Instantaneous if shared physical DB is intact. 4 to 8 hours if recovery from database backups is required. Note that multiple databases must be restored if a physical disk failure occurs. There can be up to 10 BCE site-specific databases on a given BCE SQL server. It is not clear that the databases can be restored in parallel. Estimated worst case to recover all 10 databases manually is 24 hours	1 - If it takes to do a full ma restore of the server and all databases then incident consu the allowed d for a year. In the worst c manual restor 10 databases, maximum of of straight dov will probably exceeded.
BCE Server Physical Disk Failure	SAN replication plus manual disk restore followed by manual database restores if necessary	If SAN is up, switch over to the replicated databases. If SAN replicates are not available, each database will have to be restored from backup.	Time to recover depends on the backup strategy. If a full backup of each database is taken every Sunday, it is possible that a full week's worth of transaction logs will be loaded. Worst case is probably 8 hours per database but the restores and be done in parallel. We can use 24 hours total to recover all databases as we did above.	As above

BCE site-specific database failure	SAN replication plus manual disk restore followed by manual database restores if necessary	If SAN is up, switch over to the replicated database. If SAN replicate is not available, the database will have to be restored from backup.	4 to 8 hours. Since only one database is involved the ability to restore in parallel is not an issue.	3 if time to re-operations is 8 hours 6 if time to re-operations is 6 hours
------------------------------------	--	--	---	--

The BCE-PPI high availability plan also has to account for limited availability or unacceptable wait times caused by performance issues. Performance can limit availability when a BCE application server cannot process incoming messages in a timely fashion or when BCE database server cannot process database transactions in a timely fashion.

Ensuring acceptable system performance is the responsibility of the DCO data center where the BCE servers are deployed. The data centers use sophisticated monitoring tools like Computer Associates Application Performance Monitor (CA APM, formerly CA Introscope) to detect slowdowns and determine what is causing the performance problem. Once a cause is determined, the system administrators can act rapidly to resize VM's, adding memory, CPU capacity, disk capacity and so on as required.

The procedures used to ensure High Availability are described in detail in the POM. In brief, BCE Database Servers are recovered using VMware, which provides the ability to automatically transfer the software execution from one VM to another to transfer a whole set of VM's from one host to another when a host goes down. BCE Application Servers do not have redundant servers and VMware automatic failover is not provided. When a BCE Application Servers fails a new server will have to be created from a snapshot and connected to its BCE site-specific database manually. The assumption is that BCE application server failure will be rare so that the overall system availability of 99.7% can be maintained using this manual procedure.

HA, failover, DR and COOP are the responsibility of the hosting organization. . Failover is a platform/hosting concern more than it is an application aspect. Failover strategies can be implemented at the VM/platform Operational System (OS) level with little to no impact to the application. Capacity/Performance testing was testing conducted by SDE because they are the responsible party for platform level engineering.

The combination of redundant hardware, real-time system monitoring, automatic failover and server reprovisioning just described will ensure that the system is available 99.7% of the time as required by the non-functional requirements for BCE-PPI Transfusion Verification.

As with most PD deployments BCE PPI Transfusion Verification has relied on SDE to design for high availability, scalability, disaster recovery and continuity of operations. The increment will also rely on DCO personnel to execute the AITC High Availability, Continuity of Operations (COOP) and Disaster Recovery (DR) plans as needed. This applies to all of the systems in the integrated solution: Vista instances, VBECS instances and the BCE application and database servers.

3.3.2. Special Technology

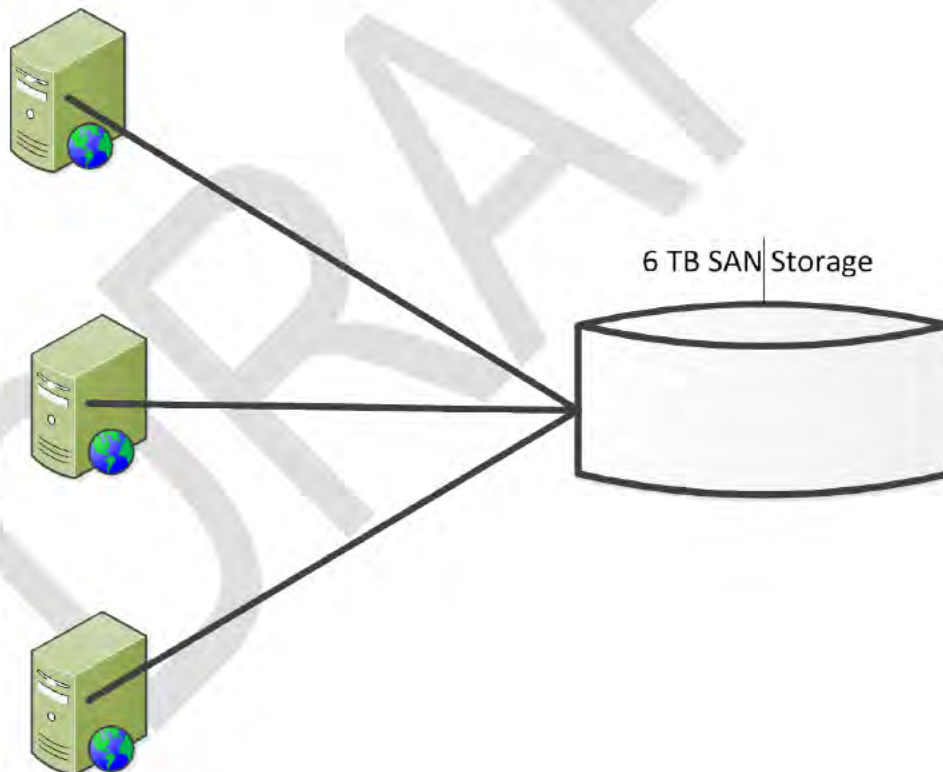
The only special technology for this increment is the CF EDA devices. The specification for those devices has been sketched earlier in this document and need not be repeated here.

3.3.3. Conceptual Overview of Physical Infrastructure

Figure 9 provides a conceptual overview of the physical hardware used to support the VM farms at the hosting datacenters. Note that the figure only describes the hardware used to host the CFTV servers. The hardware used to host VBECS is already in place. The hardware used to host VistA is already in place as well—in most cases the VistA servers are deployed in VM's at the RDC for the VISN.

Figure 9: Conceptual Overview of Physical Architecture (Host Hardware)

3 Vsphere Hosts Totaling 768 GB RAM

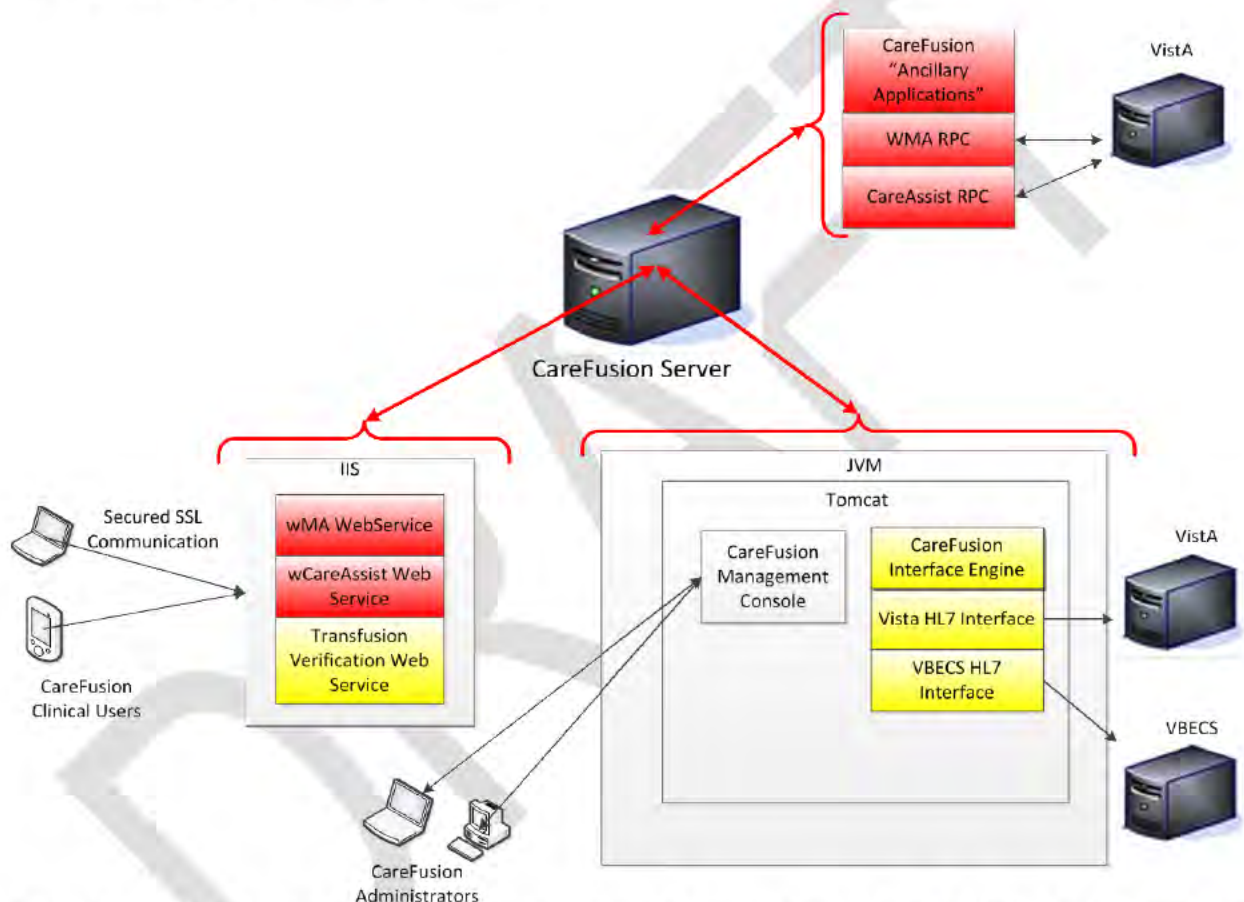


4. System Architecture

The BCE-PPI Transfusion Verification project will integrate VA VistA software, VA VBECS software, vendor CareFusion server software components (Pyxis TV, WMA and NCD), and vendor CareFusion client applications running on both EDA and desktop devices.

Figure 10 depicts the overall system architecture to be deployed at the hosting DCO datacenters (for servers) and VAMC's (for clients) during the increment.

Figure 10: CFTV VA System Architecture



As depicted in the above figure, client applications can be accessed using both the MC75AO EDA device and the wireless workstation.

Per agreement with the vendor, BCE-PPI Transfusion Verification will use the VA standard for client-server communications. The VA standard for such exchanges is to use SSL/TLS over port [REDACTED], also referred to as the HTTPS protocol.

One point of clarification needs to be made. The SSL/TLS protocol is used to transfer transfusion information from the hand-held's and workstation clients to the CareFusion Interface Engine during normal user of the system by nurses and transfusionists. This of course happens only after the client software (Operation System (OS)) and vendor application) has been downloaded onto a client in the first place. The initial download of the EDA software installation package is done using FTP. No PII will ever

be transferred to the EDA devices using FTP, however, FTP will be used down the road to update the EDAs. DCO, EO and SDE have approved the use of FTP for this purpose.

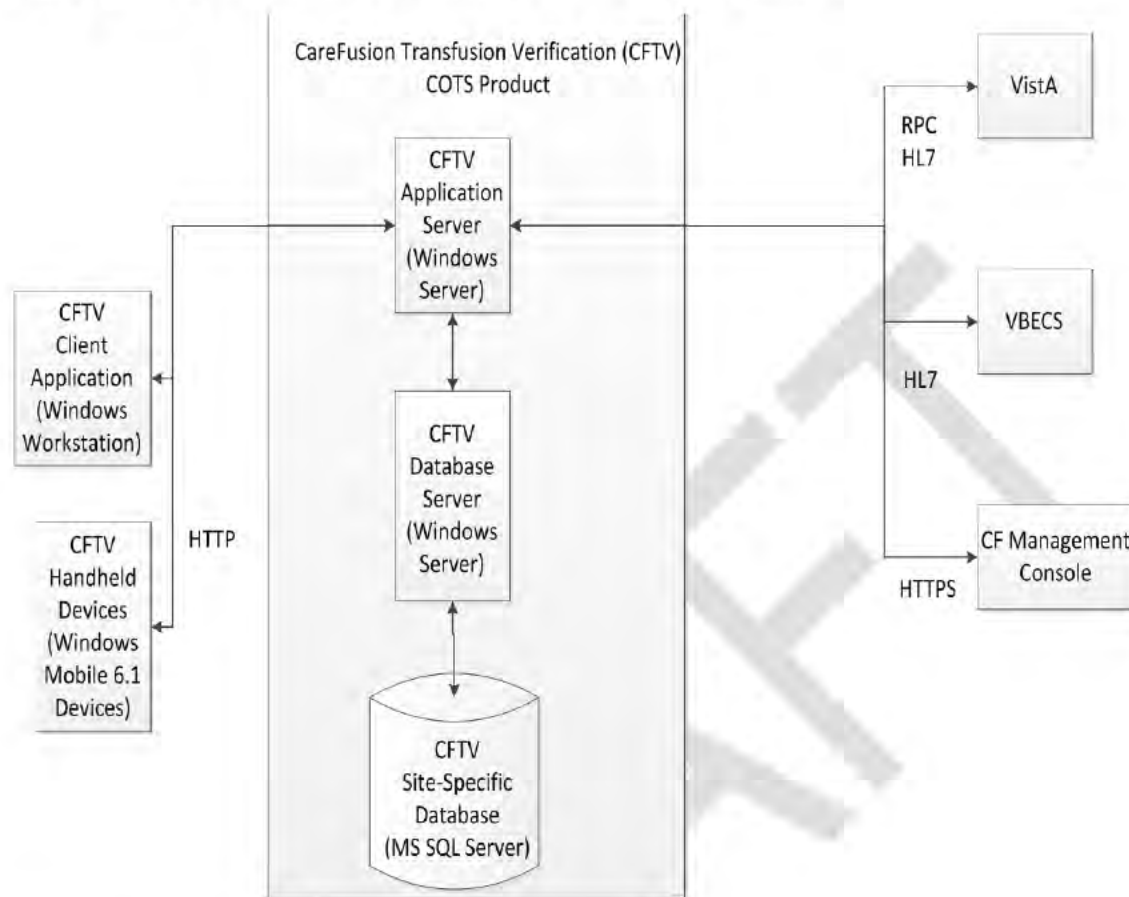
For increment 1, The BCE-PPI team delivered the Pyxis® Med Admin VA and Nurse Assist VA client applications, along with the server components on the BCE application server required to support those client applications. These applications are also known as “ancillary applications.” They are considered CareFusion legacy software because of the use of RPC architecture. Although this software interfaces with several VistA packages using RPC calls, it did not require any modification to the VistA software.

The BCE- Transfusion Verification project will build on the framework established by the ancillary applications via the release of the Pyxis® TV client applications, along with the Pyxis CareFusion server components necessary to support the client the software and interface with the other applications in the overall system including VBECS, VistA ADT, VistA Vitals and VistA TIU. The Pyxis CareFusion server components to be released for increment 2 include a Java-based interface engine, a Microsoft SQL database, and a web-client based system management application. As a part of the development effort for this increment, the VA development team has developed the VistA HL7 components necessary to communicate with the CareFusion Interface Engine (CFIE). The VA deployment team will deploy these components as a VistA patch prior to the deployment of the BCE servers for a given site. The patches which need to be installed are tabulated in section 6.2 of this document.

The actual deployment of ancillary applications during deployment of BCE-PPI Transfusion Verification. The server components of the Ancillary Applications will be installed on the BCE application server VM's used to deliver increment 2. The client applications will be installed in the images used to deliver increment 2, along with the CareFusion client software that constitutes increment 2.

The high-level system architecture for the to be deployed as BCE-PPI Transfusion Verification is shown in figure 11.

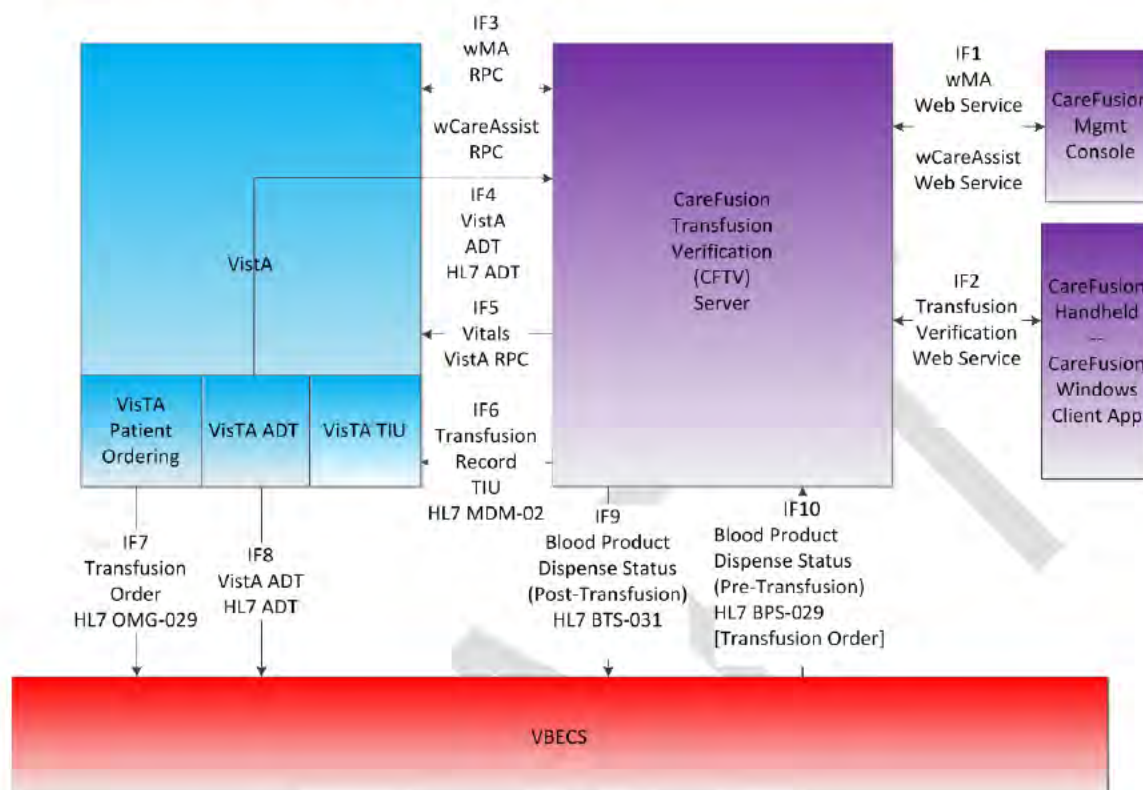
Figure 11: High-level system architecture for the BAPOC system



NOTE: Figure 11 appears in several places in this document for the readers convenience.

Figure 12 expands on the above figure, showing the interfaces depicted at a high-level (e.g. HL7) in much more detail. The HTTPS traffic between the BCE clients and the BCE application server is not broken down into individual messages. It is shown at a high level of detail.

Figure 12: Interfaces depicted at a high-level (e.g. HL7)



NOTE: Pyxis CareFusion TV client software must be installed on both the laptop (or desktop which is a second option) workstations and on the EDAs. On laptops the client application is installed using a Microsoft MSI file. Simple instructions for doing the installation have been supplied by CareFusion. They are referenced in appendix D.

The CFTV software for the EDAs is shipped as a Cabinet (CAB) file. It is expected that local support for BCE-PPI will obtain current CAB files and install them on handheld devices. A brief outline of the procedure to obtain a current CAB file appears below. (The full procedure is in the user guide for the standard Handheld Device. A reference to the Pyxis CareFusion Handheld users guide appears in Appendix D.)

1. A local support representative deletes the existing CAB file.
2. A newer version of the CAB file is automatically loaded onto the EDA from the BCE Application server.
3. The user reboots the EDA and then executes the installation procedure provided by CareFusion. This procedure is described in the Device Configuration Manual embedded below:

The deployment architecture proposed by SDE provides multiple BCE application servers (one per VistA site). The architecture also assumes that a single BCE database server will support multiple BCE application servers. Each BCE application server will connect to its own BCE site-specific database. The BCE baseline database used as a template to create the site-specific databases is not used in production.

Figure 13 shows a conventional active/passive DR solution and differs from a previous active/active F5 design with transactional replication. This is feasible because there is no need to keep the DR system perfectly synchronized with the production system. A period of manual operation is acceptable, and it is even acceptable to have manual records created during a period of manual operation which will not ever be read back in to the automated system (i.e. stored to the VistA and BCE site-specific databases) when it comes back online. Management reports and other data held in the BCE site-specific database are not lost unless the entire database is lost (which is very unlikely).

There will inevitably be fine details which will need to be worked out between DCO, EO and SDE regarding the HA and DR strategies for BCE-PPI Increment 2. However, it is important to recognize that what we have described above reflects the basic HA design of the ESE department of SDE. This HA design passed SEDR review. The following paragraphs from the SDE SDD summarize the ESE design for High Availability, which will be implemented by DCO.

To provide database high availability the vendor recommended configuration utilized Microsoft Cluster Services in an Active/Passive configuration. VA's different virtualized datacenter design plan utilizes database mirroring capabilities available in Microsoft SQL Server 2008R2. SQL Server database mirroring will provide both HA and DR for BCE-PPI databases. HA will be implemented within one datacenter (noted in this artifact as "Data Center A") through synchronous replication. If a SQL server should fail, the BCE-PPI application will be automatically directed to use the databases on the HA SQL server.

Using the same database mirroring technology, DR will be implemented through asynchronous replication between Data Center A and a second datacenter (noted in this artifact as "Data Center B"). Unlike the HA configuration, activating a DR server requires manual intervention.

4.1. **Hardware Architecture**

The vendor-supplied portion of the overall solution is comprised of system components that deploy as COTS software applications hosted on VM's. The VM's in turn are hosted on physical rack mounted servers located at the DCO. Vendor COTS applications will be load balanced at the server level using vSphere on host servers to be purchased by the BCI-PPI project, deployed within DCO and configure to support the needs of the regions. .

The VMware vSphere has been selected as the virtualization software based on its vMotion, Distributed Resource Scheduler (DRS), snapshot, and template capabilities. This aligns with the VA TRM and with VA current practice.

4.1.1. Virtual Server Configuration

The platform architecture and the number of VM's of each kind for a given region have been determined by SDE. SDE has followed the best practice of placing the BCE application server and the BCE database server on different VM's. In this regard, SDE will be following standard VA practice, which is to host database servers on separate machines to avoid having a single point of failure and to improve scalability.

The hardware configuration for BCE-PPI increment 2 appears in the SDE SDD. It is also reproduced later in this document, in the hardware detailed design section, for convenience.

The VA personnel will install and configure a VM template for both the BCE application server and the database server in accordance with vendor recommendations. For the BCE application server, the template will include MS SQL, Tomcat, Microsoft.NET, Internet Information Services (IIS), and the CareFusion Pyxis server applications ready to deploy to individual BCE-PPI sites, leaving only minimal local configuration to make the server ready for production. For the BCE database server the template will include MS SQL server software and two copies of the BCE production database. One copy will be the baseline database. The baseline database will be copied and configured for local operation, creating the BCE site-specific database for the site.

The unique post-installation steps required for each installation site are to be performed by VA field operations personnel as described in the CFTV Installation Guide. These procedures will be performed with the cooperation and sometimes the guidance of CareFusion personnel using a real-time video conferencing.

Hardware design began with a vendor-recommended hardware and software configuration for each BCE application server when it is running at a given site on physical hardware. The RAM, CPU and NIC capacity served as starting points only, they have been superseded by better numbers based on the Dallas capacity planning effort.

Table 12 shows the updated hardware parameters provided by SDE:

Table 12: Recommended minimum system requirements

System	Details
Disk Space	108GB (36GB OS/72GB data).
Processors	Dual Xeon Pentium Processors (latest model)
Memory:	4GB ECC RAM (This is load dependent and the information here is superseded by the information in the CPE report)
NIC:	1GB NIC
Platform/OS: High Availability (HA) Cluster	VMware vSphere OS: Windows 2008 Server

System	Details
Software:	<p>Database Management System (DBMS): MS SQL Server 2008 Standard or Enterprise (not used for ancillary apps)</p> <p>IIS version 6.0 or later</p> <p>Microsoft.NET version 2.0 or later</p> <p>Apache Tomcat (latest version)</p> <p>Note that two instances of Apache Tomcat are required, one to support the web services and one to support the CFMC</p>

In addition, the overall system requires that VistA and VBECS be at specific patch levels prior to being connected with the CFTV servers. Table 13 shows the required patch levels:

Table 13: Required Patch Levels

System	Details
Prerequisite VistA Software	<p>MJCF*1.0 TIU*1.0*281</p> <p>The TIU interface of the BCE-PPI integration project will allow for notes previously captured in the BTRF to be sent via the Generic TIU HL7 interface. This requires sites to have build TIU*1.0*281 which allows COTS products to upload documents into VistA CPRS via an HL7 interface without having to modify existing VistA software.</p> <p>The following links from the BCE-PPI MJCF Installation Guide section describes the steps used to:</p> <ul style="list-style-type: none"> • Verify MJCF TIU Application Parameters • Verify MJCF TIU Logical Link Parameters • Start MJCF TIU Logical Links
Prerequisite VBECS Software	<p>VBECS 1.6.1</p> <p>The technical manual, user manual and installation guide for VBECS 1.6.0 are available in the VistA Document Library (VDL). VBECS 1.6.0 provided the interface capability for the CFTV system. Version 1.6.1 is the most current version but it is not documented separately. Version 1.6.1 includes the 1.6.0 modifications.</p>

Table 14 shows the infrastructure and vendor software which will actually be used to prepare the VM template for the BCE application servers. It also shows the ports which will need to be opened and the software using the ports.

Table 14: VM Template Configuration for the BCE Application Server

System	Details
OS	Windows Server 2008 R2
Java	Java SE Update 45 or higher
Web and Application Servers	IIS 6.0 or Higher (must run in compatibility mode with IIS 6.0) Apache Tomcat 7 Update 47 or higher (for CFIE and CFMC)
Applications	Microsoft .NET Framework v2.0 or higher Microsoft .NET Framework v3.5.1 is actually in use at the test sites (Dallas, Boise and Omaha/Iowa City) Internet Explorer 7 or higher Adobe Reader 10 or higher
Vendor Server Applications (IIS Server)	CF Wireless Med Administration 5.0.2(bapiservice) CF wswCareAssistVA 2.1.4 (Nurse Data Collection – NDC) CF TV1.7.0.4 (WBCServices)
Vendor Server Applications (Apache Tomcat)	CF BASE 7.8.0.8 CF TV 1.4.0.7 VA Translation Package 1.3.1 NOTE: All these applications are assembled into one package to make CFTV_2_4_1.zip
Vendor Client Installation Packages (AirBeam)	CF Wireless Med Administration 5.0.2 CF wswCareAssistVA 2.1.4 (Nurse Data Collection – NDC) CF TV2.4.0.3
Windows Server Roles	Application Server Web Server (IIS)
Windows Server Features	Remote Server Admin Tools for Windows • Web Server (IIS) Tools Simple Network Management Protocol (SNMP) Services • SNMP Service • SNMP WMI Provider Windows Process Activation Service • Process Model • .NET Environment • Configuration APIs .NET Framework 3.5.1 Features • .NET Framework 3.5.1 • WCF Activation (Non-HTTP Activation)
Ports (Inbound)	

System	Details
Ports (Outbound)	

Note 1: CFIE – CFTV Interface Engine

Note 2: CFMC – CFTV Management Console

**VISTA RPC Broker Ports vary from site to site the convention for ports is spelled in the [Standard Specification for VMS Username and Port Numbering Conventions](#).

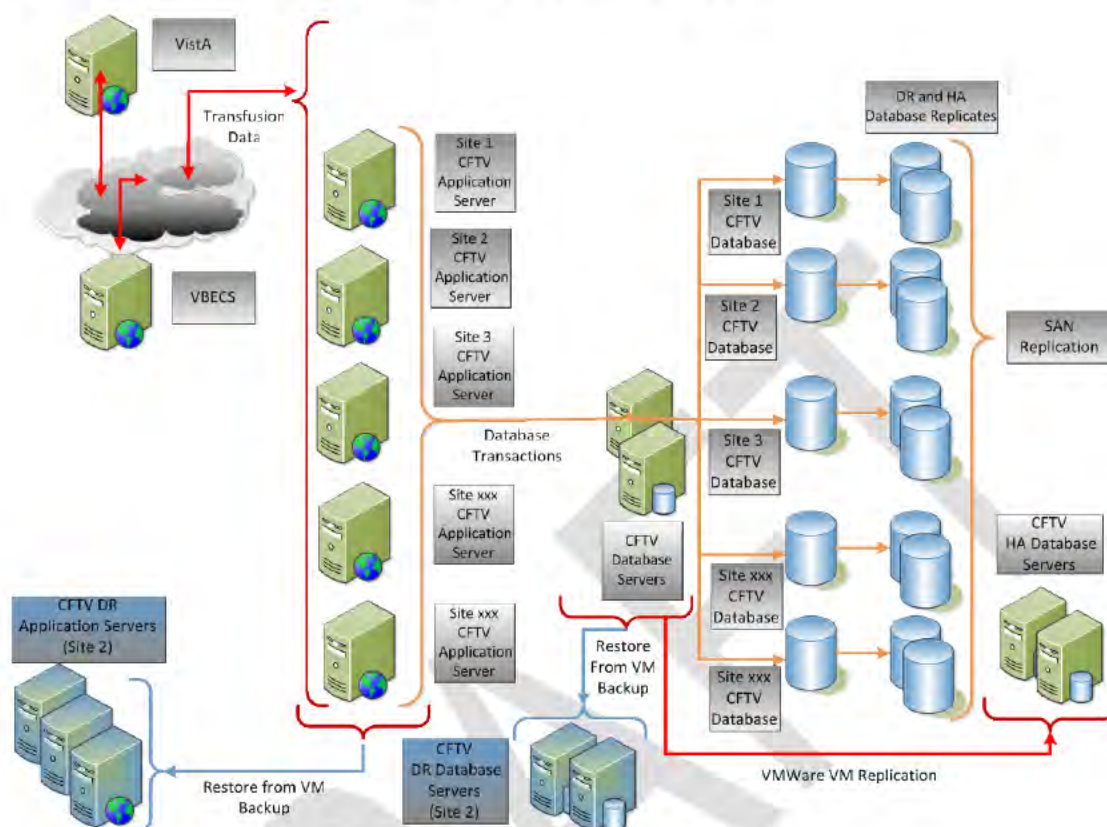
Note that the overall Blood Administration Point of Care System contains additional components which are not tabulated here. The reason is that they are hosted on the VistA and VBECS servers respectively.

4.1.2. System Deployment Logical Overview and server Side Deployment Overview

Figure 13 provides a logical view of how the system will be deployed. The figure shows multiple BCE application servers (one per VistA site). The figure also shows that a single BCE database server will support multiple BCE application servers. Each BCE application server will connect to its own BCE site-specific database. The BCE baseline database used as a template to create the site-specific databases is not used in production and is not shown in the figure. The diagram is specific to the server side; the client side has been addressed in previous diagrams. Providing and sustaining the server side virtual machines and their interfaces to VBECS and VistA is the responsibility of DCO.

- The physical servers for each medical center are identified based on a naming convention at the DCO. A BCE site requires a single BCE server and single BCE site-specific database. Note that the site-specific database need not be on a single BCE database VM and in general it is not. Ten or more site-specific databases may be hosted on a single BCE database server as long as proper care is taken to ensure that the database is mapped correctly to its application server on a one-to-one basis.
- In general a BCE database server hosts one instance of MS SQL server and if additional MS SQL servers must be added to the configuration to improve performance this will be accomplished by adding more BCE database VM's to the deployment configuration.
- There is a single VistA instance mapped to the BCE application server and the BCE site-specific database.
- Every VM instance has an associated IP address.
- DCO personnel know what site locations each BCE server supports, the VISN in which the BCE site is located, and which instance of VistA supports that BCE site location.

Figure 13: BCE-PPI Deployment Diagram (Logical System View)



Client Side Deployment Configuration:

- On the client side, there are EDA and laptop application clients.
- Each medical center needs to install the CFTV client application on the desktops of those clinicians charged with administering transfusions. At that time they must enter the IP address of the server that supports that site.
- The connection must be established between the EDA to point to the server that supports that site, and then enable the transfusion transaction with respect to the blood transfusion product.
- The project has coordinated with the vendor to streamline client interfacing and interfacing. The project has also created instructional materials and coordinated with the vendor to schedule onsite training at each site prior to deployment. Because the training materials and training courses are already in place, site clinicians and IT support personnel will be able to install, configure and support both the Pyxis TV client handhelds and the Pyxis TV desktop application.

4.1.3. Physical System Deployment Overview

This section describes how the logical design presented in the previous section will be actualized on real hardware. The first subsection shows how the system will be hosted on virtual machines in DCO-managed datacenters. BCE-PPI Increment 2 will be deployed in phases; this section describes the end state after all of the phases are finished. The second subsection describes the background processes in section 2 of this document which must be running on the BCE application and database servers in order

for the system to function. Some of these background processes come from the operating system, some come from MS SQL server and some come from the COTS vendor.

The tables in this section describe how the system will be deployed at the DCO datacenters where it will be hosted/ Since the Vista and VBECS servers are already in place, the deployment description will be restricted to the BCE servers. As noted earlier, there are two kinds of BCE servers, those which host the web services and web applications which interface with BCE clients and those which host the site-specific databases. The former are termed BCE application servers, the latter are termed BCE database servers.

The rules used in developing the deployment configuration (and in preparing the Service Level Agreement Modification (SLAM) for DCO hosting) are as follows:

1. The production environment has one BCE application server per primary site.
2. Each production BCE application server maps to exactly one BCE site-specific database. The production environment averages 1 BCE database server for every 10 BCE application VM's. This is equivalent to saying that each BCE database server hosts 10 different site-specific databases because of the 1-to-1 mapping between application servers and site-specific databases.
3. Each of the BCE database servers in the production environment is paired to an HA BCE database server. Production and HA BCE database servers are hosted at the same datacenter.
4. The pre-production test environment has one BCE application server per primary site, which is an exact replica of the production environment.
5. The pre-production test environment has one BCE database server per 10 BCE application servers. However, there are no HA servers in the test environment.
6. The DR datacenter has one BCE application VM for each BCE application VM in the production datacenter.
7. The DR datacenter has one BCE database server for each BCE server in the production data center. It also has one site-specific database for every site-specific database in the production configuration. Each production BCE database server and each production BCE site-specific database must be replicated.
8. The Salt Lake City UT, Field Office, BCE application server to be used by health product support is not assigned to a region. However, health product support will require 2 test application servers. For that reason, the SLAM calls for 132 production application servers, 132 DR application servers and 133 test application servers. HPS also has 2 Vista and 2 VBECS accounts that be created and verified to be operating correctly with the support CFTV servers.

9. All integrated sites will be supported by a primary site. For that reason, no VM's will be built for the integrated sites in any environment. There are 31 integrated sites, so the 163 total sites where BAPOC will be installed will be supported by 132 BCE application servers.

Table 15 shows the contractual physical location of the BCE application and database servers in each of the required environments. At present and per the 2013 and 2014 SLAMs, the production, HA and test servers are to be located at AITC and the DR servers are to be located at PITC.

Table 15: Physical Distribution of the CFTV (COTS) Server VM's for BCE-PPI Increment 2

CFTV Server Type	Production Server AIRC	HA Server AIRC	Pre-Production Test Server AIRC	DR Server PITC	AIRC Site Total	PITC Site Total	Grand Total
CFTV SQL Servers	14	14	14	14	42	14	56
CFTV Application Servers	132	NONE	133	132 (offline)	265	132	197
Total CFTV Servers	146	14	147	146	307	146	453

Table 16 shows the configuration of the guest VM's used for BCE-PPI Increment 2.

Table 16: Physical Configuration of Guest VM's for BCE-PPI Increment 2

Server Type	Details
CFTV Database Server VM Physical Configuration	Disk Storage: 2TB database disk 80 GB system disk RAM: 16 GB, 8 CPU vCPU's: 4
CFTV Application Server VM Physical Configuration	Disk Storage: 80GB RAM: 4GB vCPU's: 1

In order for the large collection of servers and databases involved in the BCE-PPI TV system to work together properly, there must be a mapping relating the right servers to the right partners and the right databases. The BCE-PPI Increment 2 BCE-PPI TV accomplishes the mapping task in several steps:

1. The BCE application servers have been classified by role: Production, pre-production test servers and development test servers. Each server type is identified by a three character string in the VM name for the server.
2. The BCE database servers have been classified by their VISN. The VISN number is identified by a three character string in the VM name.
3. The VM name and TCP/IP port of the partner BCE database server are entered into the configuration files on the BCE application server as described in the Installation Guide.
4. The database name of the partner BCE database is entered into the proper configuration file on the CFTV application server as described in BCE Installation Guide, along with the username for the BCE applications and the password.
5. The station ID can be used to obtain the Vista machine name and port for the Vista.
6. The VM names and TCP/IP ports for the Vista servers partnered with each BCE application server are entered into the configuration files on the BCE application server.

Most of the information needed to perform the mapping above is summarized in what is referred to as the "Server Naming Conventions Spreadsheet." The spreadsheet actually contains the region, VISN, Vista station ID and location (city and state) of all of the application servers to be deployed for BCE-PPI Increment 2. It also contains the CFTV database server name and database name for the site-specific database for that application server. In sum, the naming convention spreadsheet contains much more than conventional names. It is actually a deployment mapping table, containing almost all of the information required to deploy the system during the phased rollout, and almost all of the information needed to configure individual BCE application and database servers as they are brought into production.

NOTE: There is only development test BCE database server. It hosts site-specific test databases for each of the four test sites (Boise, Dallas, Omaha and Salt Lake City, Field Office). Since future release of the CareFusion Software will need to be field tested against the various VA systems (VBECS, Vista, ADT, TIU, etc.) and the Pyxis TV clients the test BCE database server will be relevant for a long time.) Also, the test servers should not be confused with the pre-production or production servers which will still be required. The link below points to a working copy of the server naming conventions spreadsheet, which is also the deployment mapping and configuration table.

The DCO Server Naming Conventions for BCE-Revised can be accessed by clicking the link below:

[http://\[REDACTED\]](http://[REDACTED])

Note that the above link is secured because the naming convention spreadsheet contains proprietary VA information such as server names and IP addresses which cannot be released to the public.

NOTE: The server naming conventions spreadsheet includes the database names which are only provided for the four development test servers.

4.2. Software Architecture

The software components to be delivered during increment 2 of the BCE-PPI project include a mixture of COTS developed software components from CareFusion and VA developed VistA and VBECS components.

Table 17 provides a list of the COTS products that will be implemented during increment 2 and the VA system or package which interfaces with the COTS software. Note that the Ancillary Applications (wMA and wCareAssistVA) were announced during increment 1, but they were never deployed nationally. Sites which started using the Ancillary Applications used them as class III applications and these class III applications will not be updated until Increment 2 is deployed.

NOTE: Table 17 only includes the top-level COTS components. The many web services required to support operation of the CareFusion application are not shown.

Table 17: Increment 1 COTS Software Installed with Corresponding VA Interfaces

CareFusion Product	VA System	Interface Type	Increment for Deployment
wMA	VistA – Bar Code Medication Administration (BCMA)	RPC	2
wCareAssistVA (NDC)	VistA – VITALS	RPC	2
Pyxis® Data View VA (wCareView CPRS)	VA Computerized Patient Records System (CPRS)	RPC	2
Pyxis® Transfusion Verification (CFTV)	VistA Authentication (logon)	RPC	2
Pyxis® Transfusion Verification (CFTV)	VistA – ADT	HL7	2
Pyxis® Transfusion Verification (CFTV)	VBECS	HL7	2
Pyxis® Transfusion Verification (CFTV)	VistA-TIU	HL7	2

For this increment of the BCE-PPI project the VA development teams has developed VistA components that will implement the HL7 interface with the BAPOC COTS product. The components developed include additions to the VistA HL7 messaging system and additions to VistALink. The exact nature of the modifications and instructions for developing them are giving in the MJCF Installation Guide for the increment and will not be described further here. The MJCF installation guide is available here:

[http://\[REDACTED\]](http://[REDACTED])

Table 18 shows the required patch levels for VistA and VBECS. Both systems must be patched to the required level prior to the BCE-PPI Transfusion Verification deployment.

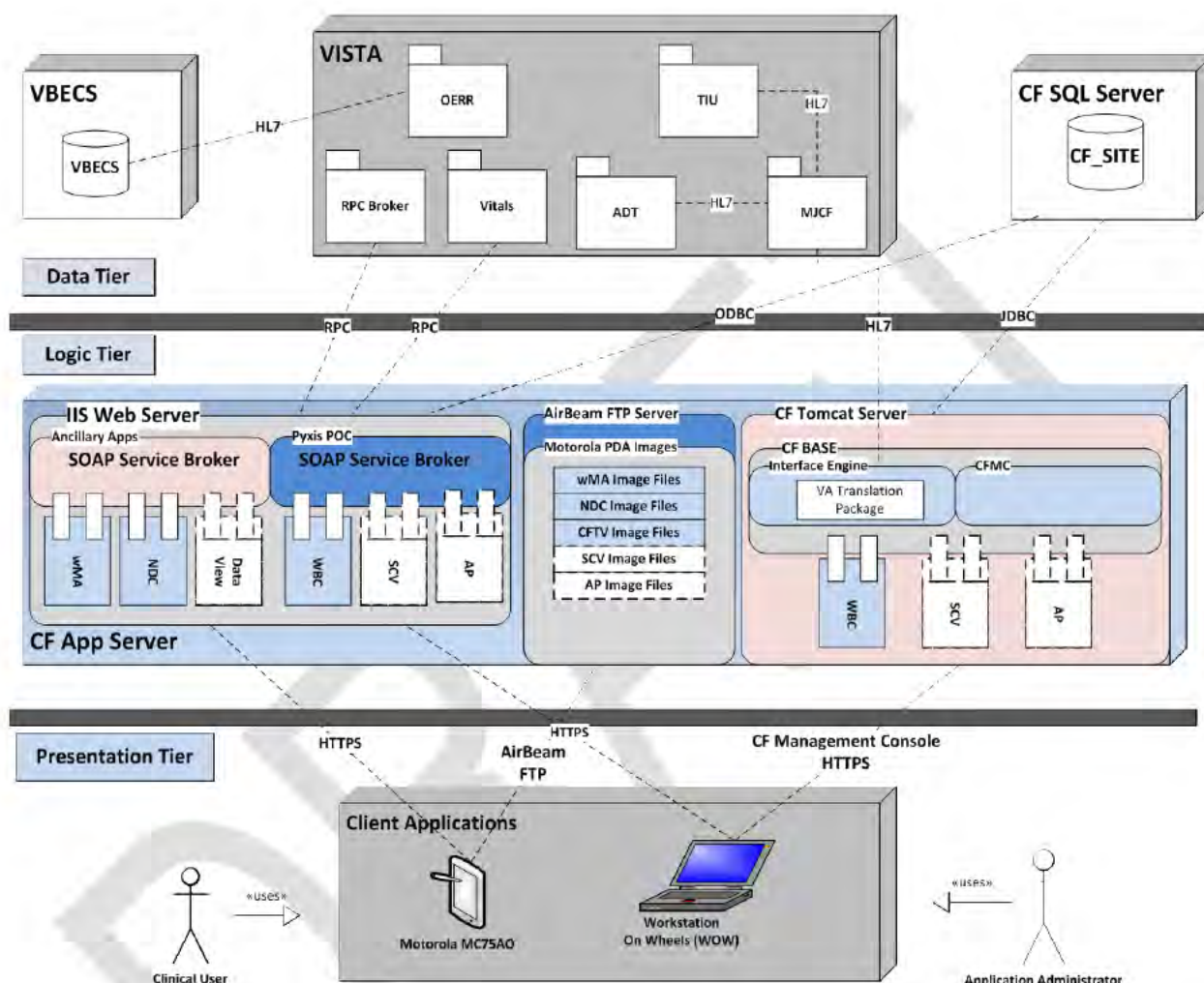
Table 18: VistA and VBECS required patch levels

System Component	Description
Prerequisite VistA Software	<p>MJCF*1.0 TIU*1.0*281</p> <p>The TIU interface of the BCE-PPI integration project will allow for notes previously captured in the SF-518 BTRF to be sent via the Generic TIU HL7 interface. This requires sites to have build TIU*1.0*281 which allows COTS products to upload documents into VistA CPRS via an HL7 interface.</p> <p>The MJCF Installation Guide has the following sections which describe the steps used to:</p> <ul style="list-style-type: none"> • Verify MJCF TIU Application Parameters • Verify MJCFTIU Logical Link Parameters • Start MJCFTIU Logical Links <p>A link to the MJCF Installation Guide is provided below:</p> <p>http://[REDACTED]</p>
Prerequisite VBECS Software	<p>VBECS 1.6.1</p> <p>The Technical Manual, User Manual and Install Guide for VBECS 1.6.0 are available in the VistA Document Library (VDL)</p> <p>http://[REDACTED]</p> <p>Technically, the prerequisite is really version 1.6.0 which included the BCE COTS Interface. The current version however is 1.6.1</p> <p>There is not a Technical manual for 1.6.1 the version 1.6.0 is the most current</p>

System Component	Description
	<p>Technical Manual and has the BCE COTS Interface information</p> <p>In practice version 1.6.1 can be installed because it includes the 1.6.0 fixes and the manual for version 1.6.0 can be used.</p>

Figure 14 shows the overall software architecture for the increment 2 BAPOC solution. This figure elaborates the architecture down to the component level and identifies all the CareFusion components which will be installed as part of the increment 2 deployments. It also identifies all of the VistA packages and VBECS involved in the solution. The VBECS and BCE MS SQL databases are shown, but the VistA Multi-User Multi-Programming System (MUMPS) database is not. The CareFusion “ancillary components” described previously are shown, as are the RPC calls which interface the ancillary components to VistA.

Figure 14: BCE-PPI Increment 2 Software Component Architecture



The above architecture diagram also provides an overview of the interfaces in the BCE-PPI increment 2 solution. Interface types are indicated on the line connecting the two interface elements.

- HTTPS indicates the secure hypertext transfer protocol. All of the interfaces between the Pyxis Carefusion Software components running on the BCE Application Server and the CareFusion Pyxis Clients rely on HTTPS request/response interchanges. This includes the Ancillary Applications (WMA and NDC). As the figure indicates the clients interact with the server software over HTTPS by calling SOAP service endpoints exposed by the CareFusion SOAP Service brokers.
- RPC Indicates a Remote Procedure Call. The Pyxis CareFusion Software relies heavily on Vista remote procedure calls to obtain data from Vista. One primary interface relying on RPC is the

Vitals exchange. The authentication process also relies of VistA RPC's to transmit the access and verify codes for a user to VistA and to receive login permission in return. Finally, the authorization process also relies on RPC's.

- HL7 indicates the use of a standardized HL7 message. These messages are in detail in section 7.
- ODBC indicates the use of the Open Database Connectivity Standard to interface between applications and databases. In this case the ODBC interfaces are between CFIE and the BCE site-specific database.

Table 19: Component Abbreviations and Names

Component Abbreviation	Component Name
VistA Components	
CPRS	Computer Patient Record System (Graphical User Interface for VistA)
TIU	Text Information Utility
MJCF TIU HL7	CFTV to VistA TIU HL7 interface (VistA Side)
VistaLink XML	VistALink Java-to-M interface with XML message exchange
RPC Broker	Remote Procedure Call Broker (Interface between CPRS and the VistA MUMPS code and database)
Kernel	Process Manager and Scheduler for VistA
Vitals	VistA Vital Signs Management Package
BCMA	Bar Code Medication Administration
ADT	VistA Admission Discharge and Transfer Package
MJCF ADT HL7	CFTV to VistA ADT HL7 Interface (VistA Side)
VBECS Components	
VBECS VistALink Listener	VistALink Java-to-M interface
VBECS HL7 MultiListener	VBEC HL7 listener with the ability to listen for messages from multiple sources
CareFusion Server Components	
CF Tomcat Instance	Apache Tomcat, a Server for Java Server Pages (JSP's) which can also serve as a web server
CFIE	CFIE- A Web Application which provides an HL7 interface between CF Web Services and other components of the system
wswCareAssistVA	Interface with the VistA Vitals Package
BAPIService	Broker API service (interfaces with the VistA RPC broker)
WBCService	Wireless Blood Care service – Interfaces with the CFTV application on the clients, including the
WCCService	Interfaces with the CF specimen collection clients. This must be installed on the server for the WBCService to work because that service depends on WCCService.
wMAService	Interface with VistA Barcode Medication package Administration (BCMA)
CareFusion Client Components	
MedAdmin (also known as WMA)	Wireless Medication Administration
NurseAssist (also known as NDC)	NDC
CFTV	An abbreviation for the Pyxis TV application. It stands for CareFusion Transfusion Verification. (These terms are used synonymously throughout this document.)

Because VBECS plays such a central role in the software architecture for BCE-PPI Transfusion Verification it is important to understand how VBECS interfaces to various VistA packages. That information is available in the BCE-PPI Technical Manual (referenced in appendix D) and in section 7 of this document.

4.3. **Communications Architecture**

BCE-PPI Increment 2, Pyxis Transfusion Verification Integration will leverage existing VA network capabilities by utilizing HL7 messaging to implement communication between the CareFusion web services and the VistA and VBECS systems.

Figure 15 shows the HL7 messaging sequence that increment 2 will employ. It also spells out the exact messages which are exchanged in the process of verifying a transfusion.

Figure 15: Communication Architecture

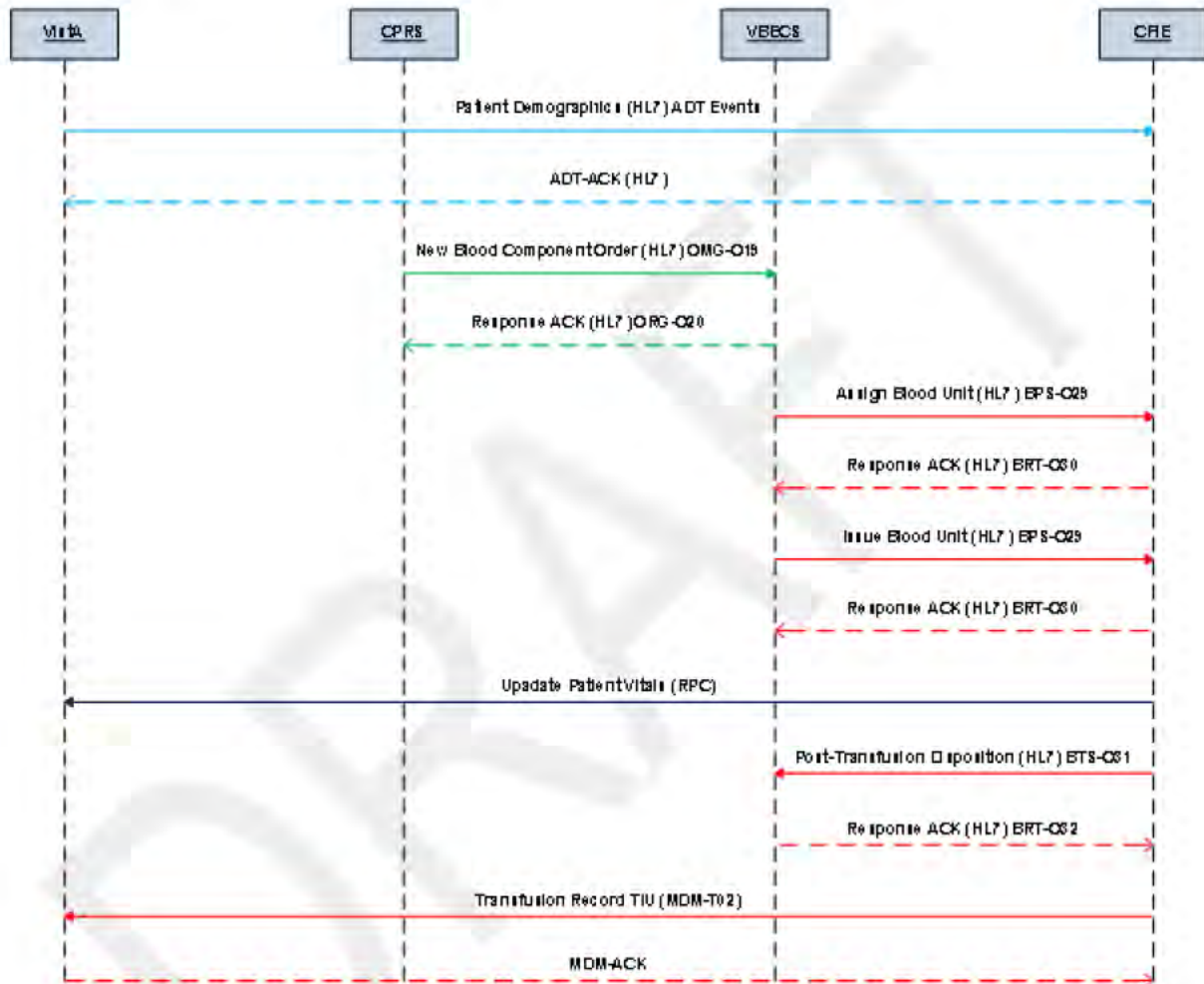
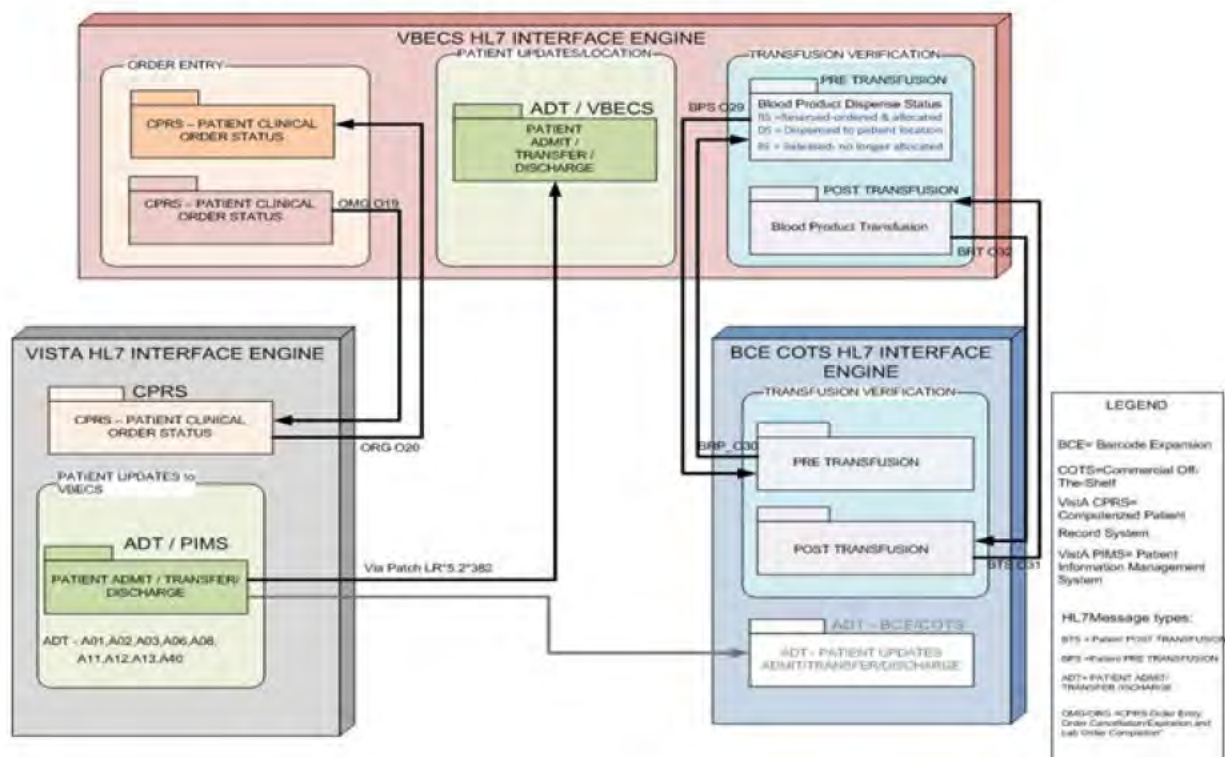


Figure 16: BCE-PPI Expansion VBECS HL7 Messaging Context Diagram



The External Interface design section of this document (section 7) provides additional detail on the communication architecture and specifics for both the HL7 and RPC interfaces.

5. Data Design

5.1. Database Management System Files

The VistA software components delivered with this Increment do not require a new dedicated data repository. The existing VistA database will be used as-is. Existing VistA applications will process HL7 messages and continue to store the data in the fields where it is currently stored.

5.1.1. Site-Specific Database

The vendor CareFusion Pyxis Transfusion Verification Interface Engine (CFIE) requires a dedicated data Relational Database Management System (RDBMS) hosted on a Microsoft SQL Server 2008 platform. The MS SQL Server hosts a site-specific database for each VistA 'primary site'.

This site-specific database is used to support several functions:

1. It stores the system configuration information which is not held in the configuration files.
2. It stores data required to support the operation of the Transfusion Verification product. For example, it stores transfusion orders.
3. It provides space for composing HL7 messages.

The structure and content of the SQL database are completely proprietary. Required post-installation SQL updates for the BCE database server will require vendor involvement. The procedures for engaging the vendor are spelled out clearly in the support plan section of the Product Operations Manual (POM) (section 7).

NOTE: The following is for information purposes only. The vendor is responsible for the final configuration of the databases and runs these SQL queries.

The following SQL queries are run to update the BCE site-specific database in the process of executing a transfusion. Specifics on these queries are proprietary:

CFTR_QUEUE_TRANSFUSION_TIU_MESSAGE.sql,

CFTR_TRANSFUSION_UPDATE.sql,

CFTR_QUEUE_OUTBOUND_TRANSFUSION_VITALS.sql,

CFTR_QUEUE_OUTBOUND_EDIT_TRANSFUSION.sql

5.1.2. Scripts required to connect the CFTV application and database servers to VISTA

To connect the BCE application server to the correct VistA, the installation must execute the following SQL script.

Update CFIE_ADM_Interface set AI_HOST = '*IP or FQDN of VistA Server*', AI_PORT = '*VistA port number*' where AI_ID = [REDACTED]

The procedure for determining the correct values to use in the above query is described in the CFTV Installation Guide.

5.1.3. Scripts required to connect the BCE application and database servers to VISTA

To connect the BCE application and database servers to the corresponding VBECS system the installer must run the following SQL script.

Update CFIE_ADM_Interface set AI_HOST = '*IP or FQDN of VistA Server*', AI_PORT = '*VistA port number*' where AI_ID = [REDACTED]

The procedure for executing this script and obtaining the correct values to use when executing it are described in the CFTV Installation Guide.

5.1.4. Procedure for linking an application server to its site-specific database

There is a specific order of creation which must be followed when creating a production instance of the CareFusion software.

1. The BCE database server must be created.
2. The site-specific databases must be created on the BCE database server.
3. The site-specific databases must be made truly site-specific by executing the scripts referred to above.
4. The BCE application server must be created
5. The BCE application server must be connected to its site-specific database.

The procedure for connecting the BCE application server to its application database is described in the BCE Installation Guide.

5.2. Non-Database Management System Files

The CareFusion applications hosted on the BCE Application server rely heavily on the use of IIS configuration files to make the system operational and to tailor the operation of the system to a particular installation. All of the configuration files are proprietary. However, based on experience gained during the installation of the Pyxis TV application and database servers at the test sites, we can list files which must be configured to create a running application server. The modifications which must be made to these configuration files are described in the CFTV Installation Guide provided by the PD team.

In addition the BCE application server must be connected to the site-specific database on the corresponding BCE database server using the procedure described in the BCE Application Server Installation Guide. In a nutshell, the procedure instructs the CFIE java web application not to use the default database and to use the IP address of the database server and the database name of the site-specific database instead.

Finally, the WBCServices configuration file must be changed to use the CareFusion TV special users. This is also described in the CFTV Install Guide.

6. Detailed Design

This section describes the proposed design in detail. Provide the necessary information for the development team to integrate the hardware components, write the software code, so that the hardware and software components will provide a functional product.

NOTE: Every design item should map back to the Functional Requirements Document. These should be captured in the Requirements Traceability Matrix.

A link to the Requirements Traceability Matrix (RTM) for this increment is provided in appendix A. The RTM links design components to specific requirements in the RSD. It also provides tests for each requirement.

6.1. Hardware Detailed Design

In this section, we provide enough information for the hosting provider to build and/or procure the system's hardware. The material here is excerpted from the SDE SDD and is for reference only. Since DCO will provision the VM's for the project based on recommendations made by SDE in that document. The document of records is the SDE SDD.

The hardware design for BCE-PPI Increment 2 is spelled out in detail in the SDE SDD. That document includes the details of hardware host servers and the VMware guest servers, including the I/O devices, and the relationship of the servers to each other. For the VMware guest servers, the SDE SDD provides:

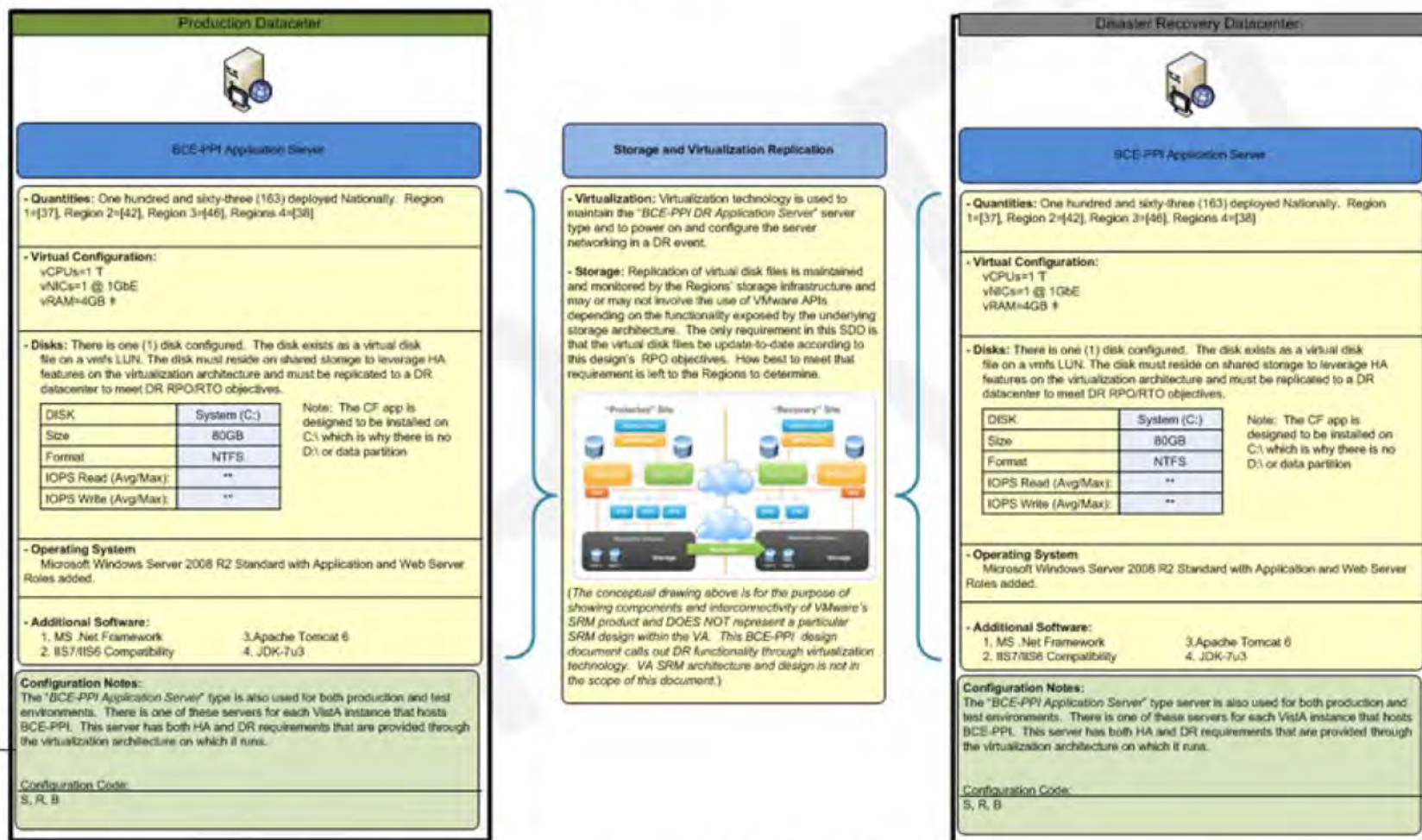
- Hard drive requirements
- Backup device requirements
- Memory and/or storage space requirements
- Processor requirements
- IP address and port information for required connections

The requirements for physical connections to the host servers including cable types and lengths, connector specifications, signal impedances and logic state are provided in the Service Contracts for the host provider, in this case DCO.

We note that an overview of all of this information has been presented earlier in this document, in section 3.

Figure 17 provides the hardware configuration for the CFTV application servers:

Figure 17: CFTV Production Application Servers Hardware Specification



* Based on Microsoft Assessment Planning Toolkit projected load at 95% or less of system resources.

** Was not part of user load testing because the disk is not used in production, is used occasionally, or has negligible load.

‡ Monitor vRAM usage and adjust as necessary.

T Monitor CPU utilization as a single processor before upgraded to a 2 processor system.

Server Configuration Codes:

B = This server requires backing up.

S = Place this server on the same datastore as other servers having identical functions to optimize de-duplication and disk block caching.

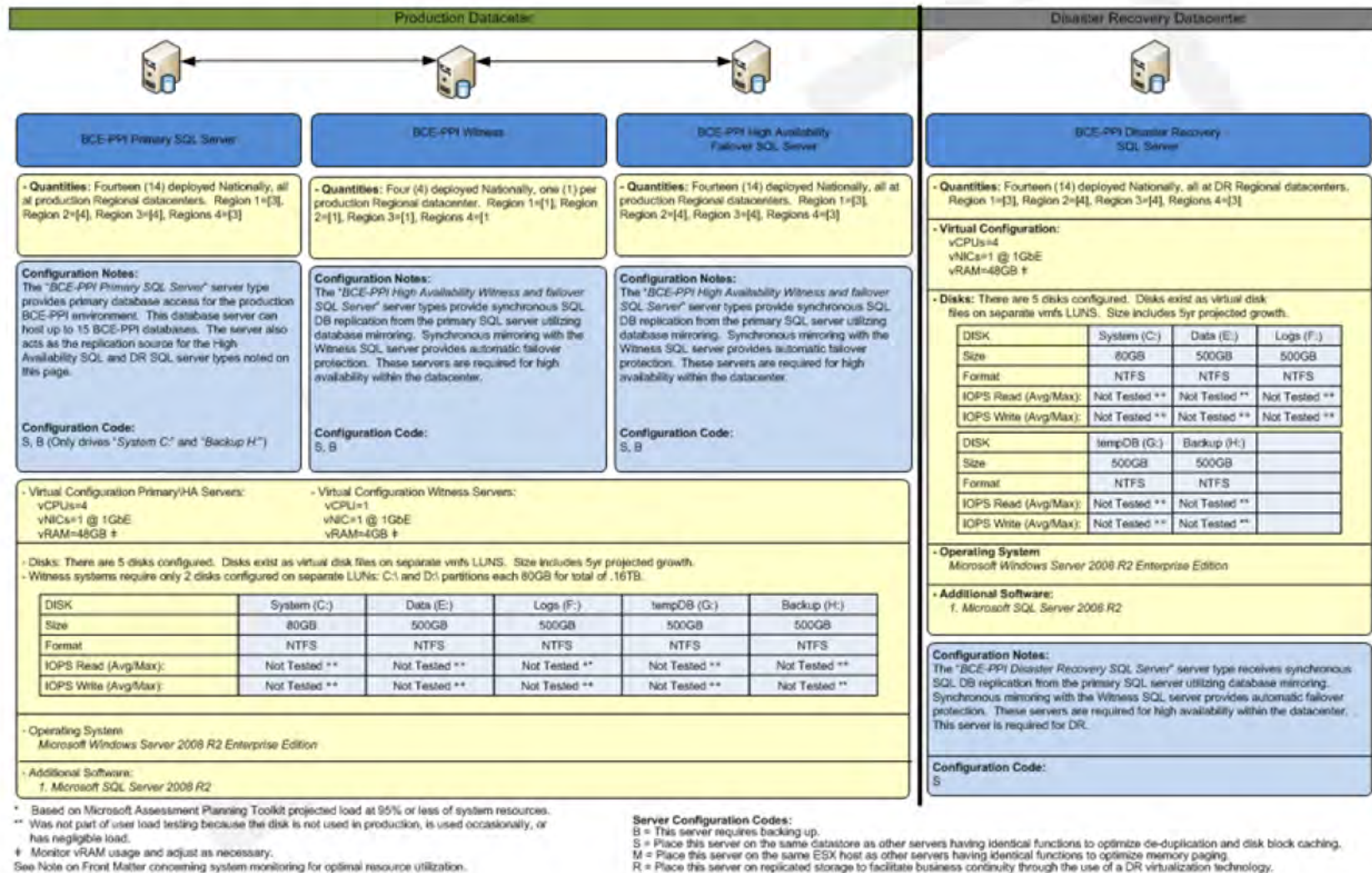
M = Place this server on the same ESX host as other servers having identical functions to optimize memory paging.

R = Place this server on replicated storage to facilitate business continuity through the use of a DR virtualization technology.

Figure 18 was taken from the SDE SDD which provides the hardware configuration for the CFTV database servers.

DRAFT

Figure 18: BCE-PPI Production SQL Server Types



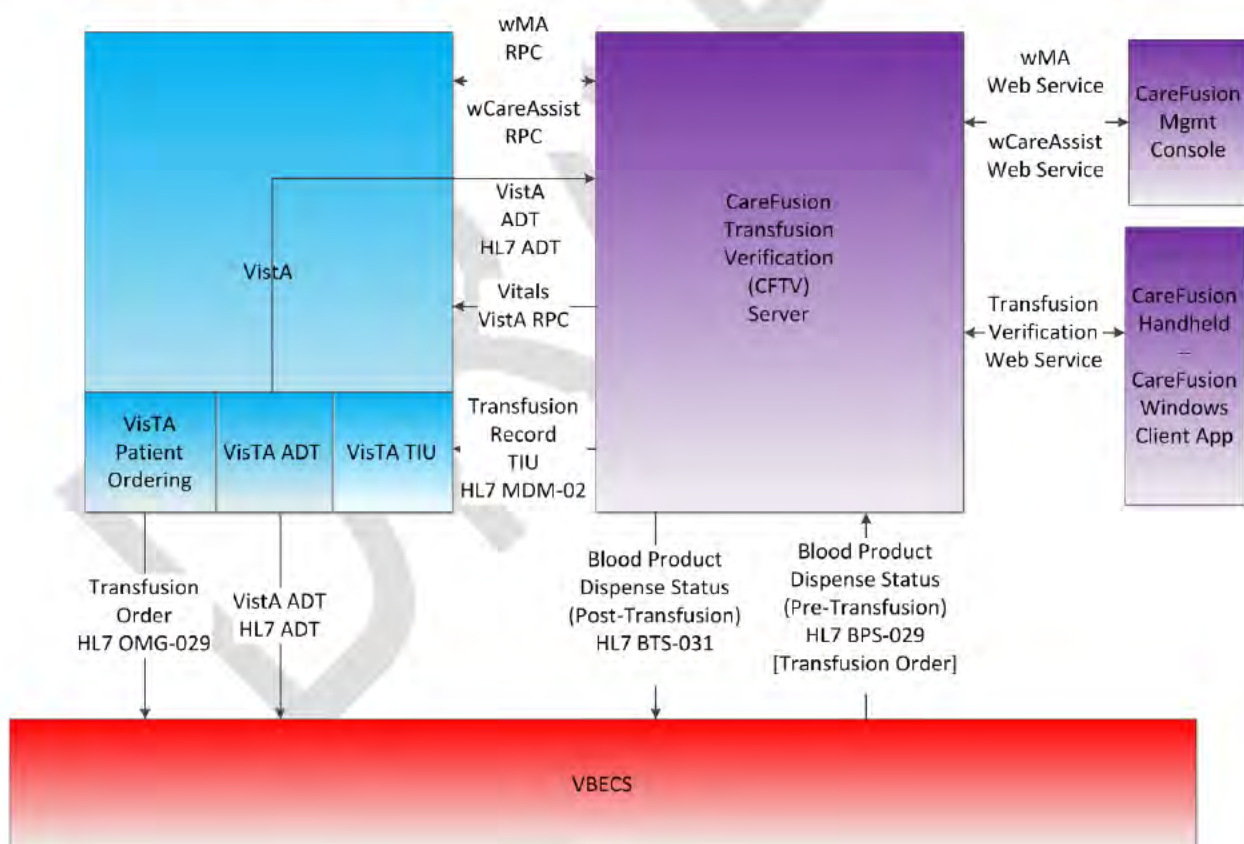
Power input requirements for each component will be provided by the hosting provider DCO based on the hardware configurations provided previously in this document and in the SDE SDD.

6.2. Software Detailed Design

For this increment of the BCE-PPI project integrates several systems with the CareFusion Pyxis TV application. The TV application forms part of the CareFusion Pyxis® PPOC suite of applications which will be implemented at all VA sites. In this section we will define the various systems that will be interfaced as part of the increment II effort and establish their systems boundaries.

The CareFusion applications will be deployed using vendor-provided clients with two form factors which transfusionists and nurses will be able to use to manage transfusion administration. Users can interact with the CareFusion applications running on a BCE application server using a mobile EDA or a client application installed on a laptop. The BCE application server interacts with the CareFusion clients, VBECS, and Vista packages to manage each blood product administration. Figure 19 shows the overall architecture of the BCE-PPI Transfusion Verification system of systems:

Figure 19: BCE-PPI Increment II Overall System Architecture and Interface Identification



As the figure shows, BCE-PPI Increment II integrates several disparate systems. Each system is part of the system of systems which provides bar code management of blood administration. In overview, the

system of systems is composed of VistA, VBECS and CFTV. However, the communications architecture shows that CFTV does not interface with VistA in a monolithic fashion. Instead, it integrates VistA packages like ADT and TIU with VBECS and CFTV. As the figure above shows, the following subsystems are involving in the overall integration:

- VistA-PIMS ADT
- VistA TIU
- VistA Patient Ordering CPRS
- VBECS
- Pyxis CareFusion Interface Engine (CFIE), also called the Interface Package
- Pyxis CareFusion Management Console (CFMC)
- Pyxis CareFusion TV Windows Client Software
- Pyxis CareFusion TV EDA Client Software

6.2.1. VISTA-PIMS ADT

The VISTA-PIMS ADT module is a package of the VISTA system that handles inpatient/outpatient admission/discharge/transfer for a given VAMC. This system will feed the CFTV application with updates on patient location and other patient information.

Table 20: VISTA-PIMS ADT

System	Details
Title	Veterans Health Information Systems Technology Architecture – Patient PIMS Admission, Discharge, Transfer (ADT)module
Abbreviation	VISTA –PIMS ADT
Version number	5.3
Release number	MJCF_1_0.KID (The use of the MJCF KIDS Package is correct)
Point of Contact	OIT Product Development VISTA
Vendor [optional]	N/A

Please refer to the VistA documentation in the VDL and on the appropriate SharePoint sites for documentation on the VistA PIMS-ADT package.

6.2.2. VISTA CPRS – TIU

The Generic TIU HL7 interface module provides COTS application with a means to upload and manage documents, which become part of the patient's records. In the BCE-PPI increment 2 integration, the

interface to the TIU system allows the CFTV application to upload the Transfusion Record Form to the patient record as a TIU document.

Table 21: VISTA– TIU

System	Details
Title	VISTA – Text Integration Utility
Abbreviation	VISTA-TIU
Version number	1.0
Release number	TIU*1.0*281
Point of Contact	OIT Product Development VISTA
Vendor [optional]	N/A

CPRS in general and the TIU package in particular are documented in the VDL and in the SharePoint sites devoted to VistA. A good starting point for learning about the TIU package is the BCE-PPI Technical Manual.

6.2.3. VistA Patient Orders

The VistA Patient Order package allows clinicians to order medications, treatments, therapies and consults. In the case of BCE-PPI increment II we are concerned with the ability to order blood products.

Table 22: VistA Patient Orders

System	Details
Title	VistA package Computerized Patient Record System (CPRS)
Abbreviation	OR (VistA Namespace)
Version number	3..0 (Current CPRS version number)
Release number	OR*3.0*309
Point of Contact	TBD
Vendor [optional]	N/A

6.2.4. Vista Blood Establishment Computer System

The VBECS is the Blood Bank re-engineered system. Blood products must be ordered through CPRS. VBECS tracks the processing and administration of the blood products.

Note that in spite of its name, VBECs is not hosted on the same servers as VistA per se, nor is it a VistA package. VBECS software is hosted on dedicated servers which may be sited either at a RDC or locally, meaning at a given VAMC.

The CFTV interface to VBECS allows the status of a blood product order to be updated based on bar code reads.

Table 23: Vista Blood Establishment Computer System

System	Details
Title	Vista Blood Establishment Computer System
Abbreviation	VBECS
Version number	1.6
Release number	VBECS 1.6.0.7
Point of Contact	Office Information Technology (OIT) Product Development VISTA
Vendor [optional]	N/A

6.2.5. CareFusion Pyxis TV System Server Software – Interface Package

The heart of the Blood Administration Point of Care solution is the CareFusion Interface Package, which the CareFusion documentation refers to as the CFIE. The CFIE is a Java web application which is hosted on the Tomcat application server.

Some additional information on the theory of operation and design of the CFIE is provided in the Pyxis TV User Guide. There is also some information about the configuration of CFIE and the BCE Application server earlier in this document (in the configuration files section). Currently this is all of the information the vendor has made available.

Table 24: CareFusion Pyxis TV System Server Software – Interface Package

System	Details
Title	CareFusion Pyxis Point of Care –Transfusion Verification
Abbreviation	CFIE
Version number	CFTV HL7 VA Interface Package 1.3.0 (Java) Java (Deployed to one of the Tomcat application servers)
Release number	1.3.0
Point of Contact	Microtech/CFTV
Vendor [optional]	CFTV

6.2.6. CareFusion Pyxis TV System Server Software – Management Console

The management console is a web application supplied as a part of CareFusion Pyxis TV which allows designated TV system administrators to configure the Pyxis TV server applications and their interfaces.

Some additional information on the theory of operation and design of the CFMC is provided in the CF Pyxis TV User's Guide. Currently this is all of the information the vendor has made available.

Table 25: CFTV BAPOC System Server Software – Management Console

System	Details
Title	CareFusion Pyxis Point of Care –TV Management Console
Abbreviation	CFMC
Version number	2.4.1
Release number	2.4.1
Point of Contact	Microtech/CF
Vendor [optional]	CF

6.2.7. CareFusion Pyxis TV System Software –Windows Client Software

The CareFusion Pyxis TV system also provides two user interfaces to the server software. One UI is a windows application which runs on a windows workstation, which typically is a laptop located near a given point of care (e.g. in a patient's room).

Table 26: CFTV BAPOC System Software –Windows Client Software

System	Details
Title	CF TV Pyxis Pont of Care –Transfusion Verification
Abbreviation	CFTV
Version number	Client App 2.4.0.3 (MSI installer)
Release number	Client App 2.4.0.3 (MSI Installer)
Point of Contact	Microtech/CFTV
Vendor [optional]	CFTV

6.2.8. CareFusion Pyxis TV System Software –EDA Controller

CareFusion also provides a EDA controller for transfusionists and nurses to use to control blood product administration. The EDA provides the same functionality as the Windows Client Application, but in a more mobile fashion.

Table 27: CFTV BAPOC System Software –EDA Controller

System	Details
Title	CFTV Pyxis Pont of Care –Transfusion Verification
Abbreviation	CFTV
Version number	Image file 2.4.0.3 – Whole OS is installed and client is overwritten
Release number	Image file 2.4.0.3
Point of Contact	Microtech/CFTV
Vendor [optional]	CFTV

6.2.9. CareFusion Pyxis TV System Software – Web Services

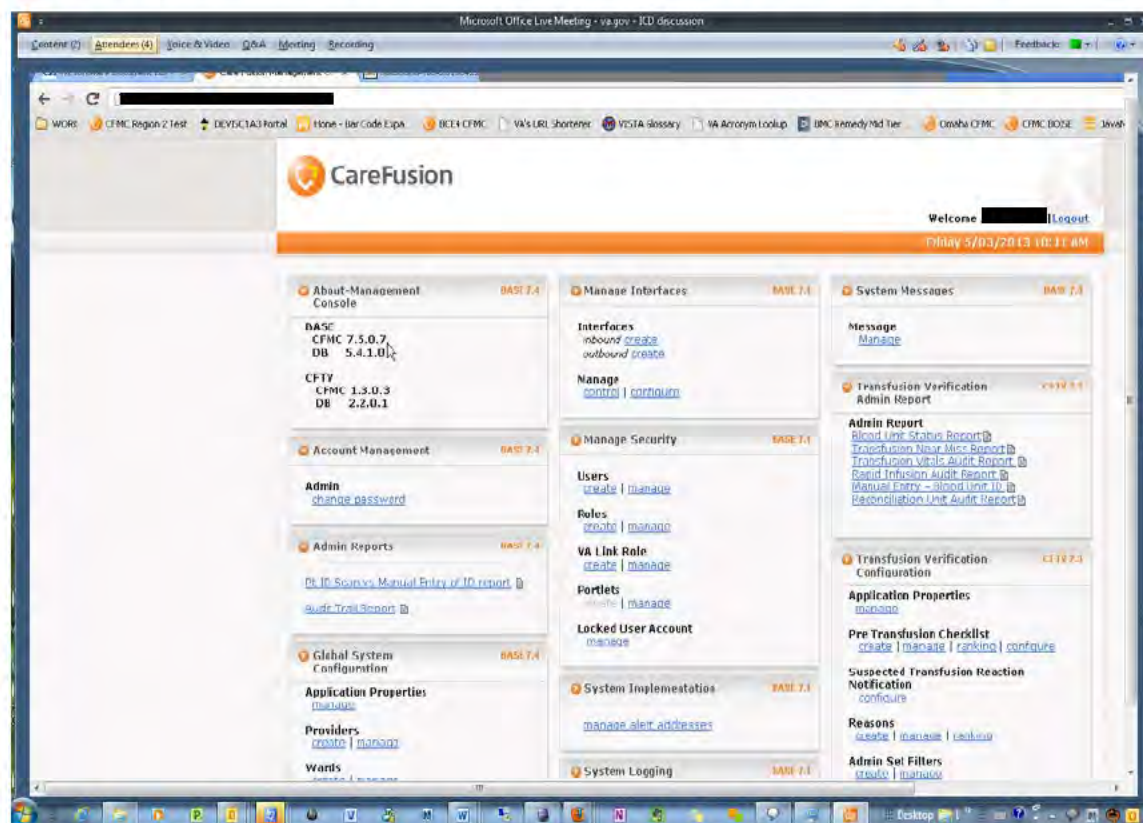
CF Pyxis provides a set of system services which transfer information from the BCE application server to the CF Pyxis TV clients.

Table 28: COTS BAPOC System Software – Web Services

System	Details
Title	CFTV Pyxis Pont of Care –TV Web Services
Abbreviation	None
Version number	WBCServices (TV) Web Service 1.6.0.3 dotNet (deployed to IIS)
Release number	1.6.03
Point of Contact	Microtech/CFTV
Vendor [optional]	CFTV

CFTV administrators and others with access to the CFTV server software can obtain version information directly from the Management Console by bringing up the main web page. The URL for the main web page and a typical set of version numbers are shown in figure 20:

Figure 20: CFTV Management Console Main Page Showing Software Versions



6.2.10. Detailed Design of the BCE Application Server

The BCE Application Server contains two web containers for use by CFTV applications and services. One of them is the server provided by Microsoft Internet Information Services (IIS). This container communicates via Transmission Control Protocol / Internet Protocol (TCP/IP) protocols with the client applications, VISTA, VBECS and SQL Server. The other web container is Apache Tomcat. A BCE application server actually has a single instance of Tomcat. This instance hosts the CareFusion Interface Engine and the CareFusion Management Console. Both the Interface Engine and the Management Console are web applications (“web apps”) written in Java.

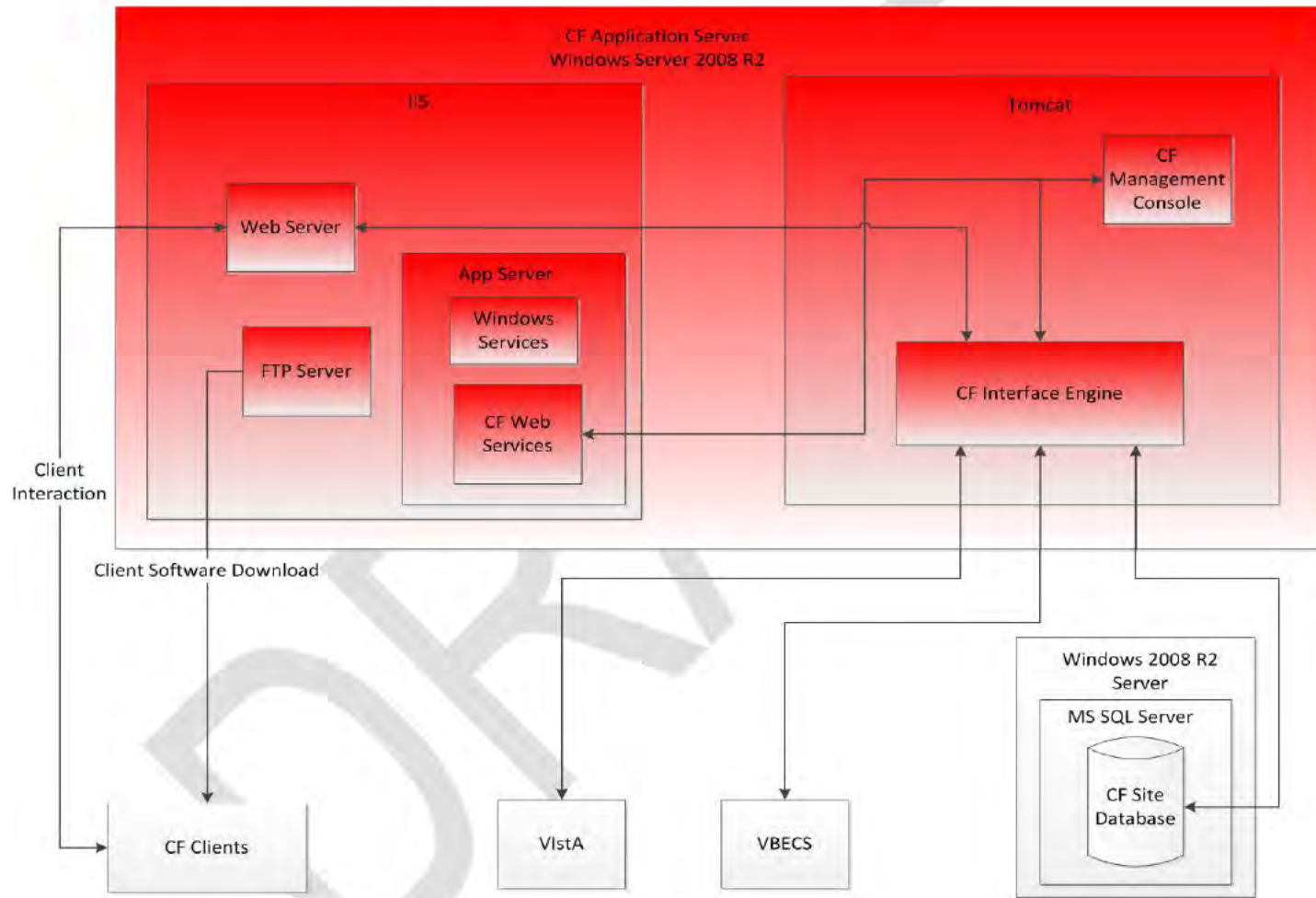
IIS and Tomcat are both “application servers” and “application containers” which provide (among many other things) a web server capability. We have avoided using the term application server term for IIS and Tomcat to prevent confusion with the use of “application server” for the entire VM we are creating, i.e. the CFTV application server. Strictly speaking a BCE application server hosts two application containers, IIS and Tomcat. The IIS hosts web services of many kinds including web services from CF Pyxis TV. As previously mentioned, the CF Pyxis web applications per se are hosted in a Tomcat container.

A Windows Server 2008 installation will install the Microsoft framework that undergirds IIS (the .Net framework) along with IIS itself. (IIS is installed when the web server role is selected for the overall windows server as described in detail below.) However, an “out of the box” IIS installation will not

support the CareFusion Pyxis TV web services so much of the “installation” procedure involves configuration of IIS. Details of the IIS configuration are supplied below.

Figure 21 shows the overall architecture of the CFTV application server and how it is installed. The components in red are installed as part of the CFTV Server Installation described in the CFTV Installation Guide.

Figure 21: CFTV Application Server Components and Relationships



As the figure shows, the CFTV Interface Engine and the CFTV Management Console are web applications which execute inside of the Tomcat Web Container. Tomcat requires a Java Virtual Machine (JVM) in order to execute. The required JVM is obtained by installing the Java Development Kit (JDK). Installing the JDK also provides numerous other capabilities which are used by both Tomcat and the CFTV applications.

The overall BCE-PPI system integration includes the interfaces with VISTA and the VBECS. Procedures on installation and configuration of those components are included in other BCE-PPI project documentation located on the project SharePoint Site. In particular they are in the MJCF installation guide.

The CFTV Web Services installation components are included in the VA_CFTV_1_0 Distribution package under the Server Setup <DIR>. The following components are included:

- **Pyxis Med Administration VA Web Service.5.0.2.0.msi**
- **Pyxis NDC VA Web Service.2.1.1.0.msi**
- **Pyxis Specimen Collection Verification Server 2.4.0.3 Web Services Installer**
- **Transfusion Verification Web Services 1.7.0.4 Installer – WBCServices.1.6.0.3.msi**
- **CareAssistVA 2.1.0.0 Web Services Installer – wswCareAssistVA.2.1.0.0.exe**

7. External Interface Design

External systems are any systems that are not within the scope of the system under development, regardless whether the other systems are managed by the development company or its client.

In this section, we describe the interface(s) between the system under development (i.e. this system) and other external systems and/or subsystem(s).

7.1. Interface Overview and Data Transfer

Figure 22 depicts the data interchange between the systems involved in the Transfusion Verification

Figure 22: BCE-PPI Increment II Interface Identification Diagram

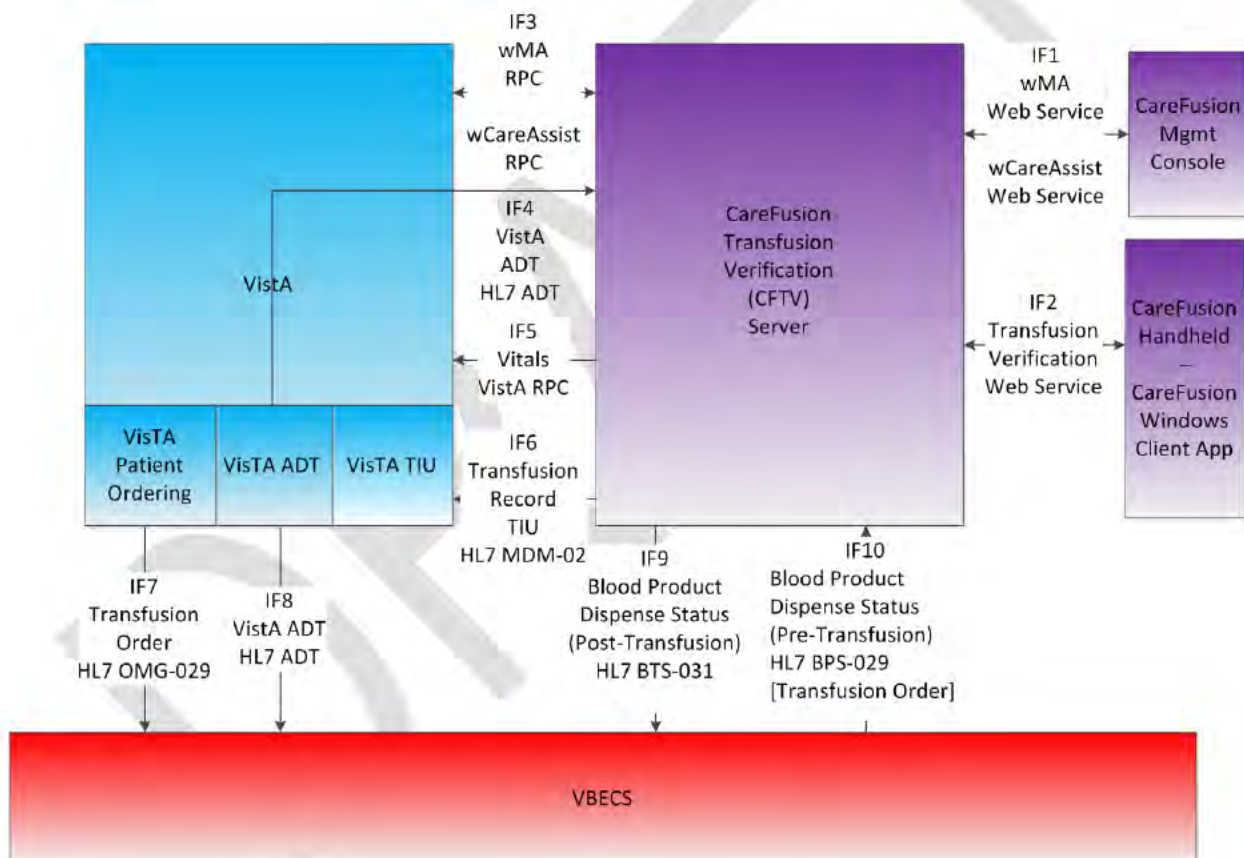


Table 29 provides the HL7 Version information, which is interface specific. In other words, while the basic interface mechanism throughout the BCE-PPI Increment II integration is HL7 version 2, different versions of HL7 are employed by different interfaces. The difference is due to different HL7 implementation in both the VistA packages and the VBECS system.

Table 29: BCE-PPI Increment II Interface Summary with HL7 Versions

Interface Designator	Systems Interfaced and Direction	Interface Mechanism	HL7 Protocol Version	HL7 Message Designator
IF4	VistA ADT to BCE App Server	HL7	2.3	HL7 ADT
IF6	BCE App Server to VistA Transfusion Record (TIU Note)	HL7	2.4	HL7 MDM-O2
IF7	VistA Patient Ordering to VBECS	HL7	2.4	HL7 OMG-029
IF8	VistA ADT to VBECS	HL7	2.3	HL7 ADT
IF9	BCE App Server to VBECS Blood Product Dispense Status (Post-Transfusion)	HL7	2.5	HL7 BTS-031
IF10	VBECS to BCE App server Server Blood Product Dispense Status (Transfusion Order)	HL7	2.5	HL7 BPS-O29

7.2. Interface Requirements

During a transfusion episode users will be able to positively match patients to blood products/components through the use of bar code identification. This will be accomplished through the use of both wireless EDA devices and laptop application clients (Windows programs) developed by CareFusion.

7.2.1. VISTA Interface Requirements

This section specifies the requirements necessary to establish and maintain communications between VISTA and the BAPOC system. It includes requirements to be satisfied by each system when sending or receiving a message. The interface between VISTA and the BAPOC system is established via a persistent or a transient (non-persistent) TCP/IP connection. Two TCP sockets provide bi-directional communications between the systems. Within the context of the TCP socket, each system will connect as the client when it initiates a message. The other system will connect as the server to receive messages from the listen state.

1. If VISTA detects a remote end disconnect, it shall attempt to reconnect to the BAPOC system TCP Server Socket for a locally defined number of Retry Attempts.
2. If VISTA detects a remote end disconnect and is unable to reconnect to the BAPOC system after locally defined number of Retry Attempts, it shall log an error.
3. If the BAPOC system detects a remote end disconnect, it shall close that channel of its TCP Server Socket and wait VISTA reconnection.
4. The Receiving system shall return an Accept Acknowledgement with a Commit Accept (CA) status to the Sending System for each incoming HL7 message in which the Message Header Segment (MSH) conforms to the following criteria:
 - The first segment is a Message Header Segment (MSH).
 - The Field Separator (MSH-1) is valued.
 - The Encoding characters (MSH-2) are valued.
 - The Sending Application field (MSH-3) contains the values LA7LAB or LA7POCn as appropriate.
 - The Sending Facility field (MSH-4) contains the VA stations number of the primary VA facility hosted on the VA system.
 - The Receiving Application field (MSH-5) contains the values LA7LAB or LA7POCn as appropriate.
 - The Receiving Facility field (MSH-6) contains the VA stations number of the primary VA facility hosted on the VISTA system.
 - The Date/time Message (MSH-7) is valued.
 - The Message Type Field (MSH-9) contains a valid message and event (when appropriate) type.
 - The Message Control ID Field (MSH-10) contains an ID.
 - The Processing ID (MSH-11) contains a valid ID.
 - The Version ID (MSH-12) contains 2.5.

- The Accept Acknowledgment Type (MSH-15) indicates a valid acknowledgment condition.
 - The Application Acknowledgment Type (MSH-16) contains a valid acknowledgment condition.
5. The Receiving system shall return an Accept Acknowledgement with a Commit Reject (CR) status to the Sending System for each incoming HL7 Message in which the Message Header Segment (MSH) fails to conform to the criteria in #4 above.
 6. The Receiving system shall return an Accept Acknowledgement with a Commit Error (CE) status to the Sending System for each incoming HL7 Message that it has not accepted for any reasons other than those requiring a Commit Reject.
 7. Upon receipt of an Accept Acknowledgment with a Commit Error (CE) status from the Receiving System, the Sending System shall institute appropriate notification actions.
 8. The Receiving System shall return an Application Acknowledgement to the Sending System for each incoming HL7 Message in which the Application Acknowledgement Type Field of the MSH Segment (MSH-16) is set to "AL".

7.2.2. VBECS Interface Requirements

The VBECS uses HL7 messaging to share information with other applications and services. These subsections describe the HL7 interfaces used by VBECS and the steps required to configure these interfaces for use. (Refer to the VBECS Application Interface Specification)

These HL7 interfaces use the VBECS INTERFACE ADMIN mail group on the Vista system to receive notifications when problems arise with delivery of messages to VBECS from Vista.

Refer to VBECS Application Interface Specification for BCE, version 2.0.

7.2.2.1. Requirements for Messages Inbound to VBECS

All VBECS Windows listener services are based on a core set of logic in the abstract class SimpleListener. Each listener inherits the core functionality. The VBECS HL7 Multi Listener Service is automatically started when the server is rebooted, or can be started manually. This service is designed to handle inbound data from all supported HL7 interfaces for VBECS.

Optionally, VBECS may be configured to use single-mode listener services, for example, if there is a problem with one of the interfaces and more in-depth trouble-shooting is required. A VBECS HL7 Listener Windows Service (single listener mode – each listener will use a unique IP address and port number as configured in the VBECS Administrator (refer to *SDD VBECS Administrator*) is automatically started when the server is rebooted, or can be started manually.

The listener receives an HL7 message, determines the type of message received and sends to appropriate parser for processing. All VBECS supported inbound messages are saved to the MessageLog table except ADT messages for patients not in VBECS.

See table 30 for VBECS HL7 Processing overview.

Table 30: VBECS HL7 Processing

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response
VistA PING message	Yes	Valid	N/A	N/A	PING response is sent immediately (if service is available).
All message types	No	N/A	N/A	N/A	Negative acknowledgement with an error message indicating the sending and/or receiving application(s) in the message are not supported by VBECS.
ADT	Yes	Validates message type and patient exists in VBECS	Patient Update HL7 Parser	Patient demographic data and/or location data is updated if VBECS does not have the most recent information.	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Negative acknowledgement (AR) with an error message is returned to sending application.</p> <p>The AR response message will contain detailed information regarding any invalid or missing required data in the HL7 message received by VBECS.</p>

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response
ADT	Yes	Validates message type and patient DOES not exist in VBECS	Patient Update HL7 Parser	N/A	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Since no in-depth processing is done on the message content (only enough to validate the patient is not in VBECS), an error here would result in no return message to the sending application. However, an email message is sent to the interface administrator (as defined in VBECS Administrator [refer to <i>SDD VBECS Administrator</i>]).</p>
ADT	Yes		Patient Merge HL7 parser	The Patient Merge HL7 parser updates the VBECS database with the patient merge event. Both patients must be in VBECS, if either the merge-from or merge-to patients do not exist in VBECS then the merge event cannot be processed.	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Negative acknowledgement (AR) with an error message is returned to sending application.</p>

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response
CPRS New Order or Cancel Order or Process Previous Lab Results	Yes	Validates message type and patient exists in VBECS	CPRS HL7 Parser	The CPRS HL7 Parser determines if the message is for a new order, cancel order or lab results. The message is then processed and the VBECS DB is updated.	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Negative acknowledgement (AR) with an error message is returned to sending application.</p>

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response
BCE Post-Transfusion Information	Yes	Validates message type and patient exists in VBECS	BCE HL7 Parser	The patient transfusion data is parsed and saved to the VBECS DB (if valid). If not valid, a negative acknowledgment message is returned to the BCE COTS application indicating the source of the problem and an email sent to the interface administrator (see <i>SDD VBECS Administrator</i>).	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Negative acknowledgement (AE or AR) with an error message is returned to sending application. AE is sent if a transfusion record was updated but another user is currently editing the record (locked). The AR code is sent for all other errors encountered.</p> <p>The AR response message will contain detailed information regarding any invalid or missing required data in the HL7 message received by VBECS.</p>

Table 31: VBECS HL7 Processing

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response
VistA PING message	Yes	Valid	N/A	N/A	PING response is sent immediately (if service is available).
All message types	No	N/A	N/A	N/A	Negative acknowledgement with an error message indicating the sending and/or receiving application(s) in the message are not supported by VBECS.
ADT	Yes	Validates message type and patient exists in VBECS	Patient Update HL7 Parser	Patient demographic data and/or location data is updated if VBECS does not have the most recent information.	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Negative acknowledgement (AR) with an error message is returned to sending application.</p> <p>The AR response message will contain detailed information regarding any invalid or missing required data in the HL7 message received by VBECS.</p>

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response
ADT	Yes	Validates message type and patient DOES not exist in VBECS	Patient Update HL7 Parser	N/A	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Since no in-depth processing is done on the message content (only enough to validate the patient is not in VBECS), an error here would result in no return message to the sending application. However, an email message is sent to the interface administrator (as defined in VBECS Administrator [refer to <i>SDD VBECS Administrator</i>]).</p>
ADT	Yes		Patient Merge HL7 parser	The Patient Merge HL7 parser updates the VBECS database with the patient merge event. Both patients must be in VBECS, if either the merge-from or merge-to patients do not exist in VBECS then the merge event cannot be processed.	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Negative acknowledgement (AR) with an error message is returned to sending application.</p>

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response
CPRS New Order or Cancel Order or Process Previous Lab Results	Yes	Validates message type and patient exists in VBECS	CPRS HL7 Parser	The CPRS HL7 Parser determines if the message is for a new order, cancel order or lab results. The message is then processed and the VBECS DB is updated.	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Negative acknowledgement (AR) with an error message is returned to sending application.</p>

Listener determines the type of message	Is message type supported by VBECS?	Listener determines validity of message	HL7 manager determines correct parser	VBECS Processing	Response
BCE Post-Transfusion Information	Yes	Validates message type and patient exists in VBECS	BCE HL7 Parser	The patient transfusion data is parsed and saved to the VBECS DB (if valid). If not valid, a negative acknowledgment message is returned to the BCE COTS application indicating the source of the problem and an email sent to the interface administrator (see <i>SDD VBECS Administrator</i>).	<p>Success: An application accept (AA) acknowledgement message is generated and returned to the sending application.</p> <p>Failure: Negative acknowledgement (AE or AR) with an error message is returned to sending application. AE is sent if a transfusion record was updated but another user is currently editing the record (locked). The AR code is sent for all other errors encountered.</p> <p>The AR response message will contain detailed information regarding any invalid or missing required data in the HL7 message received by VBECS.</p>

7.3. Hardware Interfaces

Pyxis® Point of Care Verification is a software solution that can be run on hospital hardware. There are three primary components to the Pyxis® Point of Care Verification System:

- PDA/Handheld with built in scanner; laptop, desktop or Workstations On Wheels(WOWs) with wired/wireless scanners
- Server/Interface Engine
- Pyxis® Point of Care Verification Console(CFMC) thin-client application

There are basic hospital infrastructure components required to implement any of the Pyxis® Point of Care Verification applications. Integrated Systems (IS) specific tasks/requirements include a wired and wireless network, interfaces (HL7), server configuration and installation, back-ups, anti-virus protection, patching, remote access, network printing.

Interfacing between the hospital clinical systems and Pyxis® Point of Care Verification is done through the Pyxis® Interface Engine (CFIE) – an application that resides on the Pyxis® Point of Care Verification server(s). Interfaces conform to the HL7 standard (version 2.5) using a TCP/IP socket-to-socket connection (9800 and above) and can be point-to-point and/or through a hospital interface engine. Data transmission is real-time and message traffic will be unsolicited.

The BCE-PPI, Increment II VISTA Applications/VBECS interfacing with a COTS BAPOC system is also dependent of WIR installation at the facility supported by the WIR.

7.4. Software Interfaces

The VISTA/VBECS system is interfaced with the BAPOC system. Each Pyxis® Point of Care Verification application has different interface requirements (listed below) and application specific HL7 interface specifications can be provided upon request. The common thread for all applications, however, is an inbound, real-time ADT interface required for PPID. In instances where Pyxis® Medstation RX is installed, some existing interfaces/capabilities may be used to satisfy Pyxis® Point of Care Verification interface requirements. Specific interface requirements for each application are listed below.

- ***Pyxis® Transfusion Verification***
 - Inbound ADT messages from the hospital admissions system for real-time patient census, allergy, and height/weight information* (required)
 - Inbound ORU (blood order) messages from the hospital's blood bank system showing patient transfusion assignment, disposition/release from blood bank to patient, and/or release back to inventory or waste (required)
NOTE: THIS IS NOT THE NURSING ORDER TO ADMINISTER.
 - Post transfusion completion information

All of the HL7 messages referenced in this summary of the operational sequence except the BPS and BTS messages are described in the applicable HL7 2.x standards document. (HL7 2.x refers to 2.3, 2.4, etc. as indicated in the table above). The BTS and BPS messages are described in Appendix E of this document.

7.5. Interface Detailed Design

Bar Code Expansion (BCE) Positive Patient Identification MJCF_1_0.KID package release is a Kernel Installation and Distribution System (KIDS) software release. It requires a standard VistA operating environment in order to function correctly. Prior to CFTV deployment to a VistA site, the VistA environment must be checked for having the correct packages and versions installed. The next section specifies the dependencies.

7.5.1. Interface Software Dependencies

The following patches must be installed prior to the installation of build MJCF_1_0.KID in order for the interfaces to work.

Table 32: Software Patches and Dependencies

Software	Version	Required Patches
VistA Blood Establishment Computer Software (VBECS)	1.0	VBECS*1.0*27
Text Integration Utilities (TIU)	1.0	TIU*1.0*281
VITALS	5.0	GMRV*5*26
RPC Broker	1.1	XWB*1.1*53

7.5.2. ADT HL7 Interface Elaboration

This build will release the software components necessary to implement the HL7 interface with the VistA Patient Information Management System (PIMS) Admission Discharge Transfer (ADT) package. The vendor COTS solution will rely on ADT HL7 messaging for Patient demographics and movement information. Patient demographics information will provide the key data to positively identify patients at the Blood administration POC.

7.5.3. ADT HL7 Protocols

The Patient Point of Care (PPoC) requires up-to-date information regarding patient location and status provided by the VistA ADT package. To accomplish this, the MJCF package release will import ten import ten new subscriber protocols.

The following table lists the ten new subscriber protocol names added as subscribers to the existing event drivers in order to properly route ADT messages to the PPOC system.

Table 33: Subscriber Protocol Names

Subscriber Protocol Name (new installation)	Event Driver Protocol (existing protocol)
MJCF ADT-A01 CLIENT	VAFC ADT-A01 SERVER
MJCF ADT-A02 CLIENT	VAFC ADT-A02 SERVER
MJCF ADT-A03 CLIENT	VAFC ADT-A03 SERVER
MJCF ADT-A04 CLIENT	VAFC ADT-A04 SERVER
MJCF ADT-A08 CLIENT	VAFC ADT-A08 SERVER
MJCF ADT-A08 SCHED CLIENT	VAFC ADT-A08 SCHED SERVER
MJCF ADT-A08 SDAM CLIENT	VAFC ADT-A08 SDAM SERVER

Subscriber Protocol Name (new installation)	Event Driver Protocol (existing protocol)
MJCF ADT-A11 CLIENT	VAFC ADT-A11 SERVER
MJCF ADT-A12 CLIENT	VAFC ADT-A12 SERVER
MJCF ADT-A13 CLIENT	VAFC ADT-A13 SERVER

CareFusion ADT-A01 SUBSCRIBER

NAME: MJCF ADT-A01 CLIENT **ITEM TEXT: CareFusion ADT-A01 SUBSCRIBER**

TYPE: subscriber CREATOR: BCE,DEVELOPER

DESCRIPTION: Bar Code Expansion ADT-A01 SUBSCRIBER

IDENTIFIER: CareFusion ADT-A01 SUBSCRIBER

TIMESTAMP: 62797,46067

RECEIVING APPLICATION: MJCF ADT

EVENT TYPE: A01

LOGICAL LINK: MJCFADT

RESPONSE MESSAGE TYPE: ACK

SENDING FACILITY REQUIRED?: YES

RECEIVING FACILITY REQUIRED?: YES

SECURITY REQUIRED?: NO

NAME: MJCF ADT-A01 ROUTER

TYPE: subscriber

CREATOR: BCE,DEVELOPER

RECEIVING APPLICATION: MJCF ADT

EVENT TYPE: A01

LOGICAL LINK: MJCFADT

RESPONSE MESSAGE TYPE: ACK

SENDING FACILITY REQUIRED?: NO

RECEIVING FACILITY REQUIRED?: NO

SECURITY REQUIRED?: NO

ROUTING LOGIC: D EN^MJCFHLRT("A01")

NAME: MJCF ADT-A01 SERVER

TYPE: event driver

CREATOR: BCE,DEVELOPER

SENDING APPLICATION: VAFC PIMS

TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A01

ACCEPT ACK CODE: NE

APPLICATION ACK TYPE: AL

VERSION ID: 2.3

SUBSCRIBERS: MJCF ADT-A01 ROUTER

NAME: VAFC ADT-A01 SERVER

TYPE: event driver

CREATOR: BCE,DEVELOPER

DESCRIPTION:

TIMESTAMP: 62790,54125

SENDING APPLICATION: VAFC PIMS

TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A01

PROCESSING ID: P

SUBSCRIBERS: MJCF ADT-A01 ROUTER

CareFusion ADT-A02 SUBSCRIBER

NAME: MJCF ADT-A02 CLIENT **ITEM TEXT: CareFusion ADT-A02 SUBSCRIBER**

TYPE: subscriber

CREATOR: BCE,DEVELOPER

DESCRIPTION: CareFusion

IDENTIFIER: CareFusion ADT-A02 SUBSCRIBER

TIMESTAMP: 62797,46067 RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A02 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES SECURITY REQUIRED?: NO

NAME: MJCF ADT-A02 ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A02 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: NO
RECEIVING FACILITY REQUIRED?: NO SECURITY REQUIRED?: NO
ROUTING LOGIC: D EN^MJCFHLRT("A02")

NAME: MJCF ADT-A02 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A02
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: NE
VERSION ID: 2.3
SUBSCRIBERS: MJCF ADT-A02 ROUTER

NAME: VAFC ADT-A02 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER
DESCRIPTION:

TIMESTAMP: 62790,54125 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A02
PROCESSING ID: P
SUBSCRIBERS: MJCF ADT-A02 ROUTER

CareFusion ADT-A03 SUBSCRIBER

NAME: MJCF ADT-A03 CLIENT **ITEM TEXT: CareFusion ADT-A03 SUBSCRIBER**
TYPE: subscriber CREATOR: BCE,DEVELOPER
DESCRIPTION: CareFusion ADT-A03 SUBSCRIBER
IDENTIFIER: CareFusion ADT-A03 SUBSCRIBER

TIMESTAMP: 62797,46067 RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A03 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES SECURITY REQUIRED?: NO

NAME: MJCF ADT-A03 ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A03 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: NO
RECEIVING FACILITY REQUIRED?: NO SECURITY REQUIRED?: NO
ROUTING LOGIC: D EN^MJCFHLRT("A03")

NAME: MJCF ADT-A03 SERVER TYPE: event driver

CREATOR: BCE,DEVELOPER SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A03
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: NE
VERSION ID: 2.3
SUBSCRIBERS: MJCF ADT-A03 ROUTER

NAME: VAFC ADT-A03 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER
DESCRIPTION:

TIMESTAMP: 62790,54125 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A03
PROCESSING ID: P
SUBSCRIBERS: MJCF ADT-A03 ROUTER

CareFusion ADT-A04 SUBSCRIBER

NAME: MJCF ADT-A04 CLIENT **ITEM TEXT: CareFusion ADT-A04 SUBSCRIBER**
TYPE: subscriber CREATOR: BCE,DEVELOPER
DESCRIPTION: CareFusion ADT-A04 SUBSCRIBER
IDENTIFIER: CareFusion ADT-A04 SUBSCRIBER

TIMESTAMP: 62797,46067 RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A04 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES SECURITY REQUIRED?: NO

NAME: MJCF ADT-A04 ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A04 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: NO
RECEIVING FACILITY REQUIRED?: NO SECURITY REQUIRED?: NO
ROUTING LOGIC: D EN^MJCFHLRT("A04")

NAME: MJCF ADT-A04 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A04
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: NE
VERSION ID: 2.3
SUBSCRIBERS: MJCF ADT-A04 ROUTER

NAME: VAFC ADT-A04 SERVER
ITEM TEXT: This protocol fires off of the PIMS Registration option
TYPE: event driver CREATOR: BCE,DEVELOPER
PACKAGE: REGISTRATION
DESCRIPTION: This server protocol fires when a patient is registered.
It generates a Health Level Seven (HL7) register a patient (event code A04) message.

TIMESTAMP: 62797,46067 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A04
PROCESSING ID: P ACCEPT ACK CODE: NE
APPLICATION ACK TYPE: NE VERSION ID: 2.3
SUBSCRIBERS: RG ADT-A04 TRIGGER
SUBSCRIBERS: MJCF ADT-A04 ROUTER

CareFusion ADT-A08 SUBSCRIBER

NAME: MJCF ADT-A08 CLIENT **ITEM TEXT: CareFusion ADT-A08 SUBSCRIBER**
TYPE: subscriber CREATOR: BCE,DEVELOPER
DESCRIPTION: CareFusion ADT-A08 SUBSCRIBER
IDENTIFIER: CareFusion ADT-A08 SUBSCRIBER

TIMESTAMP: 62797,46067 RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A08 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES SECURITY REQUIRED?: NO

NAME: MJCF ADT-A08 ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A08 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: NO
RECEIVING FACILITY REQUIRED?: NO SECURITY REQUIRED?: NO
ROUTING LOGIC: D EN^MJCFHLRT("A08")

NAME: MJCF ADT-A08 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER SENDING APPLICATION: MJCF ADT
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A08
PROCESSING ID: debug ACCEPT ACK CODE: NE
APPLICATION ACK TYPE: AL VERSION ID: 2.3
RESPONSE PROCESSING ROUTINE: Q
SUBSCRIBERS: MJCF ADT-A08 ROUTER

NAME: VAFC ADT-A08 SERVER
ITEM TEXT: Registration's ADT-A08 Server Protocol
TYPE: event driver CREATOR: BCE,DEVELOPER
PACKAGE: REGISTRATION
DESCRIPTION: This server protocol fires when a patient record is updated.
It generates a Health Level Seven (HL7) update a patient (event code A08)
message.

TIMESTAMP: 62797,46067 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A08
MESSAGE STRUCTURE: d PROCESSING ID: P
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: NE
VERSION ID: 2.3 RESPONSE PROCESSING ROUTINE: Q
SUBSCRIBERS: RG ADT-A08 TRIGGER
SUBSCRIBERS: VBECS ADT-A08 ROUTER

SUBSCRIBERS: MJCF ADT-A08 ROUTER

NAME: MJCF ADT-A08 SCHED CLIENT TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A08 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES

NAME: MJCF ADT-A08 SCHED ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A08 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES ROUTING LOGIC: D EN^MJCFHLRT("A08")

NAME: MJCF ADT-A08 SCHED SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER SENDING APPLICATION: MJCF ADT
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A08
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: AL
VERSION ID: 2.3
SUBSCRIBERS: MJCF ADT-A08 ROUTER

NAME: VAFC ADT-A08-SCHED SERVER
ITEM TEXT: Provides A08 updates from daily appointment list.
TYPE: event driver CREATOR: BCE,DEVELOPER
PACKAGE: SCHEDULING

TIMESTAMP: 62797,46067 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A08
PROCESSING ID: P
SUBSCRIBERS: MJCF ADT-A08 SCHED ROUTER

NAME: MJCF ADT-A08 SDAM CLIENT TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A08 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES

NAME: MJCF ADT-A08 SDAM ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A08 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES ROUTING LOGIC: D EN^MJCFHLRT("A08")

NAME: MJCF ADT-A08 SDAM SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER SENDING APPLICATION: MJCF ADT
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A08
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: AL
VERSION ID: 2.3 RESPONSE PROCESSING ROUTINE: Q
SUBSCRIBERS: MJCF ADT-A08 SDAM ROUTER

NAME: VAFC ADT-A08-SDAM SERVER

ITEM TEXT: Provides A08 updates from Scheduling event driver
TYPE: event driver CREATOR: BCE,DEVELOPER
PACKAGE: SCHEDULING

TIMESTAMP: 62797,46067 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A08
PROCESSING ID: P
SUBSCRIBERS: MJCF ADT-A08 SDAM ROUTER

CareFusion ADT-A11 SUBSCRIBER

NAME: MJCF ADT-A11 CLIENT **ITEM TEXT: CareFusion ADT-A11 SUBSCRIBER**
TYPE: subscriber CREATOR: BCE,DEVELOPER
DESCRIPTION: CareFusion ADT-A11 SUBSCRIBER
IDENTIFIER: CareFusion ADT-A11 SUBSCRIBER

TIMESTAMP: 62797,46067 RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A11 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES SECURITY REQUIRED?: NO

NAME: MJCF ADT-A11 ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A11 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: NO
RECEIVING FACILITY REQUIRED?: NO SECURITY REQUIRED?: NO
ROUTING LOGIC: D EN^MJCFHLRT("A11")

NAME: MJCF ADT-A11 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A11
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: NE
VERSION ID: 2.3
SUBSCRIBERS: MJCF ADT-A11 ROUTER

NAME: VAFC ADT-A11 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER
DESCRIPTION:

TIMESTAMP: 62790,54125 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A11
PROCESSING ID: P
SUBSCRIBERS: MJCF ADT-A11 ROUTER

CareFusion ADT-A12 SUBSCRIBER

NAME: MJCF ADT-A12 CLIENT **ITEM TEXT: CareFusion ADT-A12 SUBSCRIBER**
TYPE: subscriber CREATOR: BCE,DEVELOPER
DESCRIPTION: CareFusion ADT-A12 SUBSCRIBER
IDENTIFIER: CareFusion ADT-A12 SUBSCRIBER

TIMESTAMP: 62797,46067 RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A12 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES SECURITY REQUIRED?: NO

NAME: MJCF ADT-A12 ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A12 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: NO
RECEIVING FACILITY REQUIRED?: NO SECURITY REQUIRED?: NO
ROUTING LOGIC: D EN^MJCFHLRT("A12")

NAME: MJCF ADT-A12 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A12
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: NE
VERSION ID: 2.3
SUBSCRIBERS: MJCF ADT-A03 ROUTER

NAME: VAFC ADT-A12 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER
DESCRIPTION:

TIMESTAMP: 62790,54125 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A12
PROCESSING ID: P
SUBSCRIBERS: MJCF ADT-A12 ROUTER

CareFusion ADT-A13 SUBSCRIBER

NAME: MJCF ADT-A13 CLIENT **ITEM TEXT: CareFusion ADT-A13 SUBSCRIBER**
TYPE: subscriber CREATOR: BCE,DEVELOPER
IDENTIFIER: CareFusion ADT-A13 SUBSCRIBER

TIMESTAMP: 62797,46067 RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A13 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: YES
RECEIVING FACILITY REQUIRED?: YES SECURITY REQUIRED?: NO

NAME: MJCF ADT-A13 ROUTER TYPE: subscriber
CREATOR: BCE,DEVELOPER RECEIVING APPLICATION: MJCF ADT
EVENT TYPE: A13 LOGICAL LINK: MJCFADT
RESPONSE MESSAGE TYPE: ACK SENDING FACILITY REQUIRED?: NO
RECEIVING FACILITY REQUIRED?: NO SECURITY REQUIRED?: NO
ROUTING LOGIC: D EN^MJCFHLRT("A13")

NAME: MJCF ADT-A13 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A13
ACCEPT ACK CODE: NE APPLICATION ACK TYPE: NE
VERSION ID: 2.3
SUBSCRIBERS: MJCF ADT-A13 ROUTER

NAME: VAFC ADT-A13 SERVER TYPE: event driver
CREATOR: BCE,DEVELOPER
DESCRIPTION:

TIMESTAMP: 62790,54125 SENDING APPLICATION: VAFC PIMS
TRANSACTION MESSAGE TYPE: ADT EVENT TYPE: A13
PROCESSING ID: P
SUBSCRIBERS: MJCF ADT-A13 ROUTER

ADT HL7 Application Parameter

HL7 APPLICATION PARAMETER file (#771) entry associated:

- MJCF ADT

ADT HL Logical Link

HL7 LOGICAL LINK file (#870) associated:

- MJCFADT

7.5.4. TIU HL7 Interface Elaboration

Included in this release the BCE VistA package will also include software components interface the Transfusion Verification (TV) COTS solution with the Vista Text Integrated Utility (TIU) via HL7 interface. The TV COTS solution will capture electronically the Blood Transfusion Record Form (BTRF). This interface will utilize the TIU Generic HL7 VistA software components to send data capture by the vendor COTS solution and create a Progress Note in VistA TIU DOCUMENT file (#8925). The TV COTS solution will capture the required information to document a completed Transfusion.

TIU HL7 Application Parameter

HL7 APPLICATION PARAMETER file (#771) entry associated:

- MJCF TIU

TIU HL Logical Link

HL7 LOGICAL LINK file (#870) associated:

- MJCF TIU

7.5.5. VistA Authentication Remote Procedure Call Elaboration

Table xx contains the complete list of VistA authentication Remote Procedure Calls (RPCs) in use during a user login session on the TV COTS Management Console.

Table xx VistA authentication Remote Procedure Calls (RPCs)

RPC Name / Tag^Routine	Description
XUS SIGNON SETUP Routine: SETUP^XUSRB	Establishes the environment necessary for VistA sign-on.
XUS AV CODE Routine: VALIDAV^XUSRB	Checks if an ACCESS and VERIFY code pair is valid. Returns an array of values.
XWB GET BROKER INFO Routine: BRKRINFO^XWBLIB	Returns information regarding setup parameters of the RPC Broker in the following format: RESULTS(0) = Timeout period for handler READs.
XUS DIVISION GET Routine: DIVGET^XUSRB2	Returns a list of divisions for a user.
XUS GET USER INFO Routine: USERINFO^XUSRB2	Returns information about a user after logon in the following format: Result(0) is the users DUZ. Result(1) is the user name from the .01 field. Result(2) is the user's full name from the name standard file. Result(3) is data about the division that the user is working in. IEN of file 4^Station Name^Station Number Result(4) is the users Title. Result(5) is the Service/Section. Result(6) is the user's language choice. Result(7) is the users DTIME value.
XWB CREATE CONTEXT/MJCF TV USER Routine: CRCONTEXT^XWBSEC	Establishes context on the server, which will be checked by the RPC Broker before executing any other remote procedure. NOTE: Context is nothing more than a client/server "B"-type option in the OPTION file (#19). Hence, standard Kernel Menu Manager security is applied in establishing a context. Therefore, a context option can be granted to user(s) in the same manner as any option via the Kernel Menu Manager.

7.5.6. Vitals Remote Procedure Calls Interface Elaboration

The Pyxis® Transfusion Verification client application allows clinicians to capture patient vital signs that automatically update the VistA Vitals package during a transfusion episode. Vitals captured by the Blood

Administration Point of Care (BAPoC) solution use Remote Procedure Calls (RPCs) to record patients Vitals in the VistA GMRV VITALS MEASUREMENT file (#120.5).



REF: Additional documentation for all Vitals RPCs can be found in the “Vitals / Measurements Technical Manual and Package Security Guide” on the VA Software Document Library at:

[http://\[REDACTED\]](http://[REDACTED])

Table 5. VistA Vitals/Measurements Remote Procedure Call (RPC)

RPC Name/Tag^Routine	Description
GMV ADD VM EN1^GMVDCSAV(.RESULT,GMRVDATA)	<p>Used to enter a new Vital/Measurement record in VITALS MEASUREMENT file (#120.5).</p> <p>INPUT PARAMETER: The variable GMRVDATA data needed to create a Vital/Measurement record in the GMRV VITALS MEASUREMENT file (#120.5). The values are parsed out of the GMRVDATA variable in the GMRV VITAL MEASUREMENT file (#120.5):</p> <ol style="list-style-type: none"> 1) Date/time in FileMan internal format 2) Patient number from File #2 (i.e., DFN) 3) Vital type, a semi-colon, the reading, a semi-colon, oxygen flow rate and percentage values 4) HOSPITAL LOCATION file (#44) pointer value 5) User number from FILE 200 (i.e., DUZ), and the qualifier (File 120.52) internal entry separated by colons (e.g., 547*50:65) <p>RETURN PARAMETER: The .RESULT parameter will return a value.</p> <p>This RPC is documented in Integration Agreement</p>
GMV EXTRACT REC GETVM^GMVGETD(.RESULT,GMRVDATA)	<p>Retrieves vital records from the GMRV VITALS MEASUREMENT file (#120.5) for a selected patient given date span.</p> <p>INPUT PARAMETER: GMRVDATA, which consists of the following pieces of information:</p> <ol style="list-style-type: none"> 1) PATIENT file (#2) pointer (i.e., DFN) 2) End date of search (FileMan internal format) 3) Single vital type abbreviation (File #120.51) 4) Start date of search (FileMan internal format) <p>RETURN PARAMETER: Returns the name of the file (i.e., ^TMP(\$J,"GRPC")) containing a list of vital records for the selected patient within the defined date range.</p> <p>This RPC is documented in Integration Agreement</p>
GMV MANAGER RPC^GMVRPCM(.RESULTS,OPTION,DATA)	<p>Performs various actions such as building selection criteria, modifying package parameters.</p> <p>INPUT PARAMETERS:</p> <ol style="list-style-type: none"> a. DATA: Other data as required for the call.

RPC Name/Tag^Routine	Description
	<p>RETURN PARAMETER:</p> <p>The RESULTS variable contains the ^TMP("GMV" global array reference. The ^TMP("GMVMGR",\$J contains the results.</p> <p>The OPTION variable identifies a line label in the routine that is invoked to process the call.</p> <ul style="list-style-type: none"> Value of OPTION = GETLIST, returns a li for the file number specified. Value of OPTION = GETQUAL returns a qualifiers associated with this vital type. Value of OPTION = GETTEMP returns a input templates definitions. <p>The DATA variable contains any additional values the OPTION variable to process the call.</p> <p>This RPC is documented in Integration Agreement</p>
<p>GMV PARAMETER RPC^GMVPAR(RESULTS,OPTION,ENT,PAR,INST,VAL)</p>	<p>Sets and retrieves parameter values used by the user interface.</p> <p>INPUT PARAMETER:</p> <ul style="list-style-type: none"> OPTION: Identifies the entry point in the routine that will be invoked to process the RETURN PARAMETER) ENT: The entity value to use. See Integra Agreement 2263 and File #8989.518 for a values. PAR: The parameter value to use. See Fi for a list of parameter values. This value n with the letters "GMV" (no quotes). INST: The instance to use. VAL: Value assigned to a parameter. Val stored in File #8989.5. <p>RETURN PARAMETERS:</p> <ul style="list-style-type: none"> This remote procedure call sets and retrie parameter settings that are used in the gr interface. The entry point is RPC^GMVPAR.. It has parameters of RESULTS, OPTION, ENT, and VAL (ex: RPC^GMVPAR(RESULTS,OPTION,ENT AL). The RESULTS variable contains the resu or the location where the results can be fo The OPTION variable identifies the entry GMVPAR routine that will be invoked to p call. <p>This RPC is documented in Integration Agreement</p>
<p>GMV PTSELECT</p>	<p>Used as a method of processing a patient DFN and</p>

RPC Name/Tag^Routine	Description
RPC^GMVRPCP(.RESULT,OPTION,DFN,DATA)	<p>all warnings and notices (i.e. sensitivity or same la to the client application for processing. Also inclu log access of sensitive patients to the DG SECUR (#38.1).</p> <p>INPUT PARAMETERS:</p> <ul style="list-style-type: none"> • RESULT: This is the RPC return array va • OPTION: Contains the appropriate metho within this RPC call: <ul style="list-style-type: none"> – Value of OPTION = SELECT perform the supplied DFN (param 3) and retur notices and warnings for the DFN – Value of OPTION = PTLKUP: Logs a entry in the DG SECURITY LOG file (• DFN: Contains the DFN of the patient to p the SELECT or LOGSEC method of para • DATA: Used to pass in the option name t when logging against the DG SECURITY (#38.1). <p>RETURN PARAMETER:</p> <ul style="list-style-type: none"> • RESULTS(0)=Success or failure flag (-1 o both SELECT & PTLKUP methods. • RESULTS(1..n)=Messages to process by from the SELECT method.
GMV MARK ERROR ERROR^GMVUTL1(.RESULT,GMVDATA)	<p>Marks a selected vitals record in the GMRV VITA MEASUREMENT file (#120.5) as entered-in-error</p> <p>INPUT PARAMETER: GMVDATA 1) FILE 120.5 I #200 IEN (i.e., DUZ[number value]) set of codes i error reason.</p> <p>RETURN PARAMETER: If the record is marked a error, RESULT is set to "OK". Otherwise, RESUL "Record Not Found".</p> <p>This RPC is documented in Integration Agreement</p>
GMV TEAM PATIENTS TEAMPT^GMVUTL3(.RESULT, GMVTEAM)	<p>Retrieves patients assigned to a given team.</p> <p>INPUT PARAMETER: GMVTEAM is the internal e of the selected team (File #100.21).</p> <p>RETURN PARAMETER: Returns a list of patients specified.</p>
GMV USER RPC^GMVRPCU(.RESULT,OPTION,DATA)	<p>Retrieves data about the user (e.g., parameter se</p> <p>INPUT PARAMETERS:</p> <ul style="list-style-type: none"> • OPTION: Routine tag line to call in GMVF • DATA: Other data as required for the call <p>RETURN PARAMETERS:</p> <ul style="list-style-type: none"> • The RESULTS variable contains the resu or the location where the results can be fo • The OPTION variable identifies another e

RPC Name/Tag^Routine	Description
	<p>parameter setting) in the GMVRPCU routine invoked to process the call.</p> <ul style="list-style-type: none"> Value of OPTION = SIGNON returns information about the user who is currently signed on the system. Value of OPTION = GETPAR returns the GMV Value of OPTION DEFAULT specified in the DATA value. Value of OPTION = SETPAR will set the value of a GMV USER DEFAULT (e.g., the user's default template). <ul style="list-style-type: none"> The DATA variable contains any values not in the OPTION variable to process the call. <p>This RPC is documented in Integration Agreement</p>
GMV VITALS/CAT/QUAL GETVITAL^GMVUTL7(.RESULT,GMVLIST)	<p>Returns all qualifier information for the vital types specified in the array.</p> <p>INPUT PARAMETER: GMVLIST is a list of vital type abbreviations (File #120.51, Field #1) separated by commas (e.g., "HT^WT" for height and weight). When the value is null, all qualifier information will be returned for all vital types.</p> <p>RETURN PARAMETER: Returns the qualifier information for the selected vital types in the array specified. Includes abnormal high and low values for the vital type, if applicable.</p> <p>This RPC is documented in Integration Agreement</p>
GMV WARD PT WARDPT^GMVGETD(GMRWARD)	<p>Lists patients registered on a particular MAS ward.</p> <p>INPUT PARAMETER: GMRWARD contains the name of the ward from Ward Location file (#42).</p> <p>RETURN PARAMETER: Returns the name of the ward containing the list of patients on the selected ward. The return value is ^TMP(\$J,"GMRPT"). If there are no patients on the ward, the global array is undefined.</p>
GMV CHECK DEVICE CHKDEV^GMVUTL2(GMVIEN,GMVDIR,GMVRMAR)	<p>KERNEL utility used to return a list of printers the user can select to print output (maximum of twenty entries).</p> <p>INPUT PARAMETERS:</p> <ul style="list-style-type: none"> GMVIEN: The value to begin the search in the printer file (#3.5). Can be null. GMVDIR: Direction of the search (1 = forwards, -1 = backwards). If DIR is null, then set to 1. GMVRMAR: Right margin as a single number or a range (e.g, 80, 132 or "80-132"). <p>RETURN PARAMETER: RESULT(n)=P1^P2^P3^P4^P5^P6^P7^P8^P9^P10^P11^P12^P13^P14^P15^P16^P17^P18^P19^P20</p>
GMV CLINIC PT CLINPTS^GMVCLIN(CLIN,BDATE)	<p>Lists patients who have an appointment for a selected clinic and a given period of time.</p> <p>INPUT PARAMETER:</p> <ul style="list-style-type: none"> CLIN: CLIN contains the name of the selected clinic from the Hospital Location file (#44).

RPC Name/Tag^Routine	Description
	<ul style="list-style-type: none"> • BDATE: BDATE contains TODAY, TOMORROW, YESTERDAY, PAST WEEK or PAST MONTH <p>RETURN PARAMETER: Returns a list of patient DFNs for the selected clinic and the given date span in the array specified.</p> <p>RETURN PARAMETER DESCRIPTION: Returns patient names and DFNs for the selected clinic and date span in the array specified.</p>
GMV CLOSEST READING CLOSEST^GMVGETD(.TEST,GMVDFN,GMVDT,GMVT,GMVFLAG)	<p>Returns the observation date/time and reading of closest to the date/time specified for the patient a</p> <p>INPUT PARAMETER:</p> <ul style="list-style-type: none"> • GMVDFN: A pointer to the Patient (#2) file • GMVDT: The date/time to search from. T NOW. • GMVT: The vital type abbreviation as it appears in FILE 120.51, Field 1 (e.g., WT). • GMVFLAG: A flag to indicate if the search is before or after the date/time specified in t value where 1 indicates before, 2 indicates after, and 3 indicates either direction. <p>RETURN PARAMETER: Returns a string composed of two pieces. The first piece contains the observation date/time (File #120.5, Field .01) of the record that was found. The second piece contains the rate (File #120.5, Field 1.2) of the record. If there is an error, the first piece will be -1 and the second piece will be the error text.</p>
GMV CONVERT DATE GETDT^GMVGETQ(.RESULT,GMRDATE)	<p>Converts a user-supplied date/time into VA FileMan internal and external date format.</p> <p>INPUT PARAMETER: GMRDATE is the user-supplied date/time text.</p> <p>RETURN PARAMETER: .RESULT, Date in internal FileMan format^Date in external FileMan format</p> <p>This RPC is documented in Integration Agreement</p>
GMV CUMULATIVE REPORT EN1^GMVSC0	<p>Prints the Cumulative Vitals Report.</p> <p>INPUT PARAMETER: GMVDATA: A multi-piece variable that identifies the values needed to run the report:</p> <ol style="list-style-type: none"> 1: DFN 2: Start date/time of the report range (FileMan format) 3: End date/time of the report range (FileMan format) 4: n/a 5: Device name (File 3.5, Field .01) 6: Device internal entry number 7: date/time to print the report (FileMan format) 8: ward internal entry number (File 42) 9: hospital location internal entry number (File 44)

RPC Name/Tag^Routine	Description
	<p>10: list of rooms separated by a comma (e.g., 200)</p> <p>RETURN PARAMETER: Returns a message status outcome of the request to queue the report. If the report is successfully queued, RESULT will be "Report sent". Task #: "ZTSK" where ZTSK is the task number of the report. If the report could not be queued, RESULT will be "Task not queued" and task the report."</p>
<p>GMV DLL VERSION DLL^GMVUTL8(.RESULT,GMVX)</p>	<p>Returns a YES or NO response to indicate if the DLL file should be used.</p> <p>INPUT PARAMETER: GMVX: This value is the name of the file and the date/time associated with it (e.g., GMV_VITALSVIEWENTER.DLL:v. 07/21/05 10:30).</p> <p>RETURN PARAMETER: Returns YES if the file could be used. Returns NO, if the file cannot be used. Returns null if the file was not found.</p> <p>This RPC is documented in Integration Agreement.</p>
<p>GMV ENTERED IN ERROR-PATIENT EN1^GMVER0</p>	<p>Prints a report of all vitals/measurements entered for the selected patient for a given date/time range.</p> <p>INPUT PARAMETER: GMVDATA: A multi-piece value that identifies the values needed to run the report:</p> <ul style="list-style-type: none"> 1: DFN 2: Start date/time of the report range (FileMan format) 3: End date/time of the report range (FileMan format) 4: n/a 5: Device name (File 3.5, Field .01) 6: Device internal entry number 7: date/time to print the report (FileMan format) 8: n/a 9: n/a 10: n/a <p>RETURN PARAMETER: Returns a message status outcome of the request to queue the report. If the report is successfully queued, RESULT will be "Report sent". Task #: " ZTSK" where ZTSK is the task number of the report. If the report could not be queued, RESULT will be "Task not queued" and task the report."</p>

7.5.7. Software Product Security

7.5.7.1. Mail Group

BCE Positive Patient Identification MJCF_1_0.KID package release exports the following mail group.

Table 34: Mail Group Description

Mail Group	Description
MJCF HL7	This mail group is for people who need to get error messages from the MJCF messaging interfaces.

7.5.7.2. Archiving

There are no application specific archiving procedures or recommendations for the BCE Positive Patient Identification software.

7.6. **Human-Machine Interface**

This section is intended to describe the Human Machine interface (i.e. user interface) relative to the user. The template is applicable to projects which develop GOTS software, e.g. Virtual Lifetime Electronic Record (VLER) or VistAWeb. For COTS integration, the user interface design is the responsibility of the vendor. The Human-Machine interface is not under VA control. CareFusion Pyxis TV has a sensible user interface which is not hard to learn and training in the use of the software will be provided as part of BCE-PPI increment 2.

There are three user interfaces for CF Pyxis TV: (1) The user interface for the workstation client, (2) the user interface for the hand-held device and (3) the user interface for the CareFusion Management Console. (CFMC) These are all documented clearly in the Pyxis Users Guides.

8. System Integrity Controls

We note that the integrity controls which restrict the loss, misuse, modification of, or unauthorized access to information that could affect the company, client, or its customers are imposed by the VA. The VA controls provider access to the CF Pyxis TV software by using the VistA credentials of the user. A user who cannot authenticate to a VistA using an access code and a verify code cannot access the BCE application or database server(s) mapped to that VistA. The security keys and secondary menu options used to control access to CF Pyxis TV functionality are described below and have also been sketched in section 2.5.4 under security and privacy requirements.

8.1. BCE-PPI System Integrity

Access to the BCE servers is controlled by the VA in the same way that access to all servers is controlled, namely by using Lightweight Directory Access Protocol (LDAP). In fact, BCE servers will be locked down enough to prevent vendor access. Management operations on BCE servers will be performed by VA system administrators. If direction from BCE support personnel is required it will be provided by giving instructions to VA personnel using audio and video conferencing.

It is normally the responsibility of the project team to ensure that the following minimum levels of control are included:

- Ability to identify audit information by user identification, network terminal identification, date, time, and data accessed or changed
- Audit procedures to meet control, reporting, and retention period requirements
- Controls to restrict access of critical data items
- Verification processes for additions, deletions, or updates of critical data

However, it is important to note several key points here:

1. The BCE Database does not store PII data (or any other kind of patient data) permanently. While the PII data remains in the BCE site-specific database it is secured by controlling access to that database. End user access is controlled using the authentication and authorization protocols described previously. This applies especially to CFMC access—only users with the MJ CFTV administrator role can possibly access PII data using CFMC. Access to the CFTV site-specific database itself (via SQL queries) is only available to DCO DBA's.
2. The CFTV site-specific database is not the system of record for any data. The systems of record are VistA and VBECS respectively. As just stated, access to the transient PII data in the CFTV site-specific database is strictly controlled using Role Based Access Control (RBAC).
3. The responsibility for user identification falls on VistA. This applies to both granting access to the system (authentication) and restricting access to data (authorization) Users log on to both EDA devices and the CFTV client application using their VA access and verifies codes.

4. All patient and order data generated in the CFTV application and stored in the CFTV database is transferred to VistA and VBECS in HL7 messages or RPC calls. The responsibility for data auditing and data verification is the VistA software and those who support VistA for a given site.

Although the final resting places for all PII data used by the Blood Administration Point of Care system are VistA and VBECS, the CFTV web application exposes PII data which has to be secured, even though it is transient. For this reason, the CFTV web application is secured in three ways:

1. The CFTV web application is not exposed to the internet at large. It is secured behind the VA firewall. IP address and server names for CFTV are not published.
2. The CFTV web application uses HTTPS and SSL certificates.
3. The CFTV web application itself is secured through the use of VistA Access/Verify Codes for user authorization.

In October 2013 the EAS testing team ran vulnerability scans on the CFTV Web application and found 12 issues. The executive summary of the NSOC WASA report on these vulnerabilities reads as follows:



During testing, twelve findings were identified: **Eight critical-risks**, **One high-risk**, **Two medium-risks**, **One low-risk**.

The first **critical-risk** finding identifies that the web application is vulnerable to reflected cross-site scripting. The second **critical-risk** finding identifies that the web application allows unauthenticated download of server files. The third **critical-risk** finding identifies that the web application does not enforce authorization on some pages. The fourth **critical-risk** finding identifies that the web application has multiple unauthenticated SOAP web services. The fifth **critical-risk** finding identifies that the web application stores unencrypted sensitive information at rest in the database and configuration files. The sixth **critical-risk** finding identifies that the web application is vulnerable to SQL injection. The seventh **critical-risk** finding identifies that the web application has weak administrative passwords. The eighth **critical-risk** finding identifies that the web application is vulnerable to blind SQL injection. The first **high-risk** finding identifies that the web application displays user password directly on pages. The first **medium-risk** finding identifies that the web service and PII are available unencrypted over HTTP. The second **medium-risk** finding identifies that the web application does not configure cookies securely. The first **low-risk** finding identifies that the web application fails to enforce strict password policy.

The project team worked with the vendor to mitigate the issues and corrections to the software were made and released the CFTV application was re-tested. Fixes for all of the vulnerabilities were verified as the following table from the 2/7/2013 NSOC report shows:

Table 35: EAS Regression Test Results for CFTV Web Application from the 2/7/2014 Report

#	Finding	Status (Fixed, Not Fixed, In Progress)	Fix Date (or Estimate d)	How it was fixed (Remediation details)	EAS Status (Open, Closed, Still Open)	EAS Date	EAS Notes
1	Web Application is Vulnerable to Reflected Cross-Site Scripting (XSS) Attacks	Fixed	17 Dec 2013	Transfusion Verification will be updated to use filter which will inspect each and every field that is submitted to the application and will remove all suspicious strings from request parameters/fields. Regex patterns will be used to implement the sanitization. HTML encoding input and output.	Closed	12-26-2013	12-26-2013: Verified that the reported XSS location has been fixed.
2	Web Application Allows Unauthenticated Download of Server Files	Fixed	17 Dec 2013	Transfusion Verification filters will be updated to prohibit access to the file system.	Closed	12-26-2013	12-26-2013: Verified fixed. I cannot pass an arbitrary file path to be downloaded.
3	Web Application does not Enforce Authorization on Some Pages	Fixed	17 Dec 2013	<p>Authorization has been enforced on the URL level.</p> <p><u>Update: 01-23-2014 (CareFusion)</u> We have added secondary checks via page level authorization above and beyond the referrer tag. There is logic within the code of each page, per NSOC recommendation, to verify authentication within the code. This solution is in addition to the header check already provided.</p>	Closed	2-7-2014	<p>2-7-2014: Fixed. Authorization is enforced on the page.</p> <p>12-26-2013: (Downgraded to High Finding. Vista authorization is required). The vendor implemented a check for the HTTP header “Referrer” only. Regular users of the application can still access administrative pages by adding an HTTP header “Referrer” tag to the HTTP request.</p>

#	Finding	Status (Fixed, Not Fixed, In Progress)	Fix Date (or Estimated)	How it was fixed (Remediation details)	EAS Status (Open, Closed, Still Open)	EAS Date	EAS Notes
							<p>Example HTTP Request (Logged in as regular user):</p>  <p>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referrer:</p> 
4	Web Application has Multiple Unauthenticated SOAP Web Services	Fixed	17 Dec 2013	On initial authentication of a user with the VistA system, if the user is authorized, they will be provided a session token. This token will be used for all future calls to the web services. Any service call without a token request will be rejected.	Closed	12-26-2013	12-26-2013: Verified that the WCC service is no longer active in this release. You cannot reach WBC service from another machine. Nurse data collection and wireless mediation administration require session IDs now.
5	Web	Fixed	17 Dec	Response to CFAP_PATIENT table: cell	Closed	12-26-	12-26-2013: Closed.

#	Finding	Status (Fixed, Not Fixed, In Progress)	Fix Date (or Estimate d)	How it was fixed (Remediation details)	EAS Status (Open, Closed, Still Open)	EAS Date	EAS Notes
	Application Stores Unencrypted Sensitive Information at Rest in the Application Database and Configuration Files		2013	level security using symmetric key (AES-256 algorithm) encrypted by a certificate will be used to encrypt PII data in CFAP PATIENT table. Refer to this white paper: [REDACTED] 0. The decryption password will be stored in the code and will be stored separate from the database to ensure the greatest security. Direct access to the sql database, without the password, would NOT allow access to the patient data. Direct access to the application, without the password, would NOT allow access to the patient data.		2013	
6	Web Application is Vulnerable to SQL Injection	Fixed	17 Dec 2013	Transfusion Verification has been updated to use filters which will inspect inbound data fields and will remove all suspicious strings from request parameters/fields.	Closed	12-26-2013	12-26-2013: Verified fixed.
7	Weak Web Application Administrative Password	Fixed	17 Dec 2013	Application uses VistA authentication. Password (access code/verify code) are not being stored anywhere in the database or the server. CFAP_USER table is used to store VistA user's name only. There are system accounts (sysadmin), which don't leverage VistA authentication - these accounts will be purged from the database	Closed	12-26-2013	12-26-2013: Verified fixed.

#	Finding	Status (Fixed, Not Fixed, In Progress)	Fix Date (or Estimate d)	How it was fixed (Remediation details)	EAS Status (Open, Closed, Still Open)	EAS Date	EAS Notes
				for VA installs.			
8	Web Application is Vulnerable to Blind SQL Injection	Fixed	17 Dec 2013	In addition to the filter, Transfusion Verification has been updated to use parameterized sql queries.	Closed	12-26-2013	12-26-2013: Verified fixed.
9	Web Application Displays User Passwords on Page	Fixed	17 Dec 2013	Application uses VistA authentication. Password (access code/verify code) are not being stored anywhere in the database or the server. CFAP_USER table is used to store VistA user's name only. There are system accounts (sysadmin), which don't leverage VistA authentication - these accounts will be purged from the database for VA installs.	Closed	12-26-2013	12-26-2013: Verified fixed. Vista is being used now for every account.
10	Web Service and PII Are Available Unencrypted Over HTTP	Fixed	17 Dec 2013	SSL is supported and Certificate must be provided by VA.	Closed	12-26-2013	12-26-2013: Verified fixed.
11	Web Application Does Not Configure Cookies Securely	Fixed	17 Dec 2013	SSL is supported and Certificate must be provided by VA.	Closed	12-26-2013	12-26-2013: Verified fixed.

#	Finding	Status (Fixed, Not Fixed, In Progress)	Fix Date (or Estimate d)	How it was fixed (Remediation details)	EAS Status (Open, Closed, Still Open)	EAS Date	EAS Notes
12	Web Application Fails to Enforce Strict Password Policy	Fixed	17 Dec 2013	Application uses VistA authentication. Password (access code/verify code) are not being stored anywhere in the database or the server. CFAP_USER table is used to store VistA user's name only. There are system accounts (sysadmin), which don't leverage VistA authentication - these accounts will be purged from the database for VA installs.	Closed	12-26- 2013	12-26-2013: Verified fixed. The application forces the use of Vista now.

The following table shows that all findings for the CFTV Web Application are now closed.

Table 36: CFTV Web Application findings that are now closed

REVISION DATE	REVISION NUMBER	CHANGES	AUTHOR
9/27/2013	1.0	Original	EAS END
10/7/2013	1.2	Updated with new web services listed for findings 4 & 10	EAS END
12/26/2013	2.0	Regression testing	EAS END
2/7/2014	3.0	Regression testing. All findings closed	EAS END

8.2. CareFusion Pyxis TV Access Control

Access control for BCE-PPI Transfusion Verification will be managed using VistA. This process may be summarized as follows:

1. Every CFTV user accesses the CFMC and the clients using their own VISTA access code and verify code. This includes both administrators and clinical end users. The BCE-PPI Increment 2 POM contains a detailed section on how authorization (logon) works and a detailed discussion on how to troubleshoot the problem of denied access. By design, a user's BCE account is his or her VistA account. This applies to both CFTV and to the Ancillary Applications.
2. The roles granting a user a given level of access to the CFTV software are granted based on the user's VistA access. The roles granted and the corresponding VistA access appear in table 38:

Table 37: CFTV Security Roles and Corresponding VistA Access

USER ROLE	Transfuses	VISTA Menus Option	VISTA Security Keys	Client Application Access	CFMC Access
RN	Yes	MJCF TV USER	MJCF TV USER	Yes	N/A
Nurse Manager	Yes	MJCF TV USER MJCF TV REPORTS	MJCF TV USER	Yes	TVAdmin Report TVReports
Nurse Manager	No	MJCF TV REPORTS	N/A	No	TVAdmin Report TVReport
BCE Coordinator	Yes	MJCF TV USER MJCF TV ADMINISTRATOR	MJCF TV USER	Yes	TVAdmin Report TVReports TVConfiguration

USER ROLE	Transfuses	VISTA Menus Option	VISTA Security Keys	Client Application Access	CFMC Access
BCE Coordinator	No	MJCF TV ADMINISTRATOR	N/A	No	TVAdmin Report TVReports TVConfiguration
System Administrator	NO	MJCF TV APP ADMIN	N/A	No	Access to all Portlets on CFMC

- The EDA's rely on an AirBeam Client to synchronize client software updates with the application server via FTP. This requires the setup of a local user account on the application server that only has access to the C:\inetpub\ftproot folder. For more information on how the AirBeam Smart Client works and the Symbol AirBeam package builder reference the vendor documents which can be accessed by clicking the links provided below:

- AirBeam Smart Client Reference Guide:

<http://>

- AirBeam Smart Package Builder Reference Guide:

<http://>

- The CFTV applications do not require specific AD groups to control access to its application as it relies on the VISTA RPC Broker security architecture, as well as roles defined within its own application database. VISTA will perform the function of the authorization database providing both authentication and authorization services. The CFTV application establishes role-based access control (RBAC) by defining which roles are authorized accesses to specific resources (portlets). The bullets below specify how User authorization and authentication function for both the TV Client application and CFMC web client application.

- Transfusion Verification Client Application (Desktop and EDA's):
 - User Authentication – User VISTA Access/Verify code.
 - User Authorization – User must be assigned VISTA MJCF TV USER key and MJCF TV USER secondary menu.

- CFMC Web Client (Internet Explorer):
 - User Authentication – User VISTA Access/Verify code.
 - User Authorization – Role-based access control by the VISTA secondary menus assigned to a particular user (see table 29 above for details on roles and VISTA menus).

NOTE: Although User Authentication functions similar for both applications user authorization for the CFMC web client application is more complex due to the number of roles and resources restricted by the RBAC policy.

As noted above, the people who manage VistA user accounts for a given site will be managing BCE users at the same time. The process followed for adding a VistA user or modifying a VistA users access level is already in place. A given VistA site may elect to have one person manage this process for BCE but we believe that implementing that process is the prerogative of a specific VistA site.

9. Requirements Traceability Matrix

Per the PMAS template, every SDD should include or reference a Requirements Traceability Matrix (RTM) that traces modules and data structures to the software requirements. The RTM for BCE-PPI Increment 2 has been posted to the SharePoint site and can be accessed with the proper permissions by clicking the link below:

[http://\[REDACTED\]](http://[REDACTED])

10. Packaging and Installation

There are some special considerations for software packaging and installation of the CFTV software which we sketch here. Details for the CFTV application server software is provided in the CFTV Installation Guide for Increment 2. Some detail for database server packaging and installation are provided in the CFTV Installation Guide which is available in the project SharePoint site and can be accessed by clicking the link below:

[http://\[REDACTED\]](http://[REDACTED])

Details for application server packaging and installation are provided in the CFTV Installation Guide which is also available in the SharePoint archive referred to above.

11. Design Metrics

The critical design metrics for this increment are the performance metrics. As noted earlier, these were not provided in the RSD. We have also noted that the key design metric used to undergird Dallas testing, capacity planning and hardware design is a very rough estimate and is arguably too conservative.

12. Required Technical Documents

Per the PMAS SDD template the following documents must be submitted with the SDD in order to obtain SDD approval. Based on the fact that our project is a COTS Integration, we have reviewed this list for applicability and made some changes. We have also determined that the need for some documents is conditional and we explain those conditions below.

- Product Architecture Document
- Disaster Recovery Plan
- Interface Data Mapping
- Security Assurance Strategy
- PAD – The requirement to produce a separate Product Architecture Document (PAD) has been relaxed. Projects may satisfy the PAD requirement by submitting completed product architecture sections in the SDD. This is exactly what our increment has done. The required architectural information appears in this document in the system architecture sections.

- DR and COOP – The BCE servers for BCE-PPI Increment 2 are Virtual Machines which are hosted on servers that run in data centers provided by DCO. Recovery of the VM's themselves and recovery of the infrastructure software running on those VM's is the responsibility of the data center. The BCE-PPI Product Operations Manual (POM) provides details on DR and COOP. A reference to the POM appears in Appendix D. The Information System Contingency Plan prepared by DCO forms the basis of the DR/COOP strategy.

Restoring the operation of VistA and VBECS is the responsibility of the site that uses the CFTV software. For example if VistA and VBECS are hosted on VM's and if the data center hosting the Iowa City VAMC VistA and the Iowa City/Omaha blood bank goes offline, it is the responsibility of the hosting center to provide redundant VM's, transfer operation of the VistA and VBECS software to those redundant (backup) VM's and restore VistA and VBECS to operation once the backup VM's are brought online—now as the primary VM's. In the case that VBECS is not hosted on a VM, which is currently the applicable case, the responsibility for restoring VBECS operation still falls on the VBECS staff in cooperation with National Support.

Since this is the case, the responsibility of the BCE-PPI team with respect to DR and COOP is limited. The BCE-PPI team must describe how the functionality of the COTS software is to be transferred to backup machines (which become primary machines) and how that software is to be started up and operated normally once the backups are online. Again, this information appears in the POM.

Based on the need to restore operability of the BCE server hardware and software for both disaster recovery and continuity of operations, the project team has a separate facility DR Plan and a BCE-PPI COOP. However, the picture here is complicated by the fact that the BCE-PPI team is not responsible for the transfer of BCE server hardware functionality to backup servers or the transfer of infrastructure software operation. Those responsibilities fall on hosting center personnel. Additional details are provided in the POM and a reference to the POM appears in appendix D. The DR/COOP plan for AITC (using PITC) is described in the Information System Contingency Plan (ICSP) for BCE-PPI.

The BCE-PPI team is responsible for ensuring that the CF Pyxis TV software can be restarted on the backup servers after they become primary. The BCE-PPI team is also responsible for providing information that allows the hosting center team to recover from common errors. However, this information already appears in the POM for BCE-PPI Increment 2. The POM covers normal startup, normal operation and recovery from common errors. We will also describe how startup, normal operation and error recovery differ when they occur as a result of a disaster or a loss of hardware or software functionality.

- Security Documentation – The BCE-PPI COTS software is currently classified as a major application. One consequence is that we are required to obtain an ATO prior to deployment of the software to production. Another consequence of the major application status is that we are required to prepare or submit the security documents which would be used to support accreditation and the resulting ATO.
- Interface Data Mapping – Documenting the data presented by the user interface and how that data is presented applies to projects where the team is actually developing the GUI software. This documentation requirement is not applicable for COTS integration projects and for that reason we have not provided an Interface Data Mapping Document.

- IT Infrastructure Standards
- Systems Engineering and Design Review (SEDR) process
- Enterprise Architecture Web page
- One-VA TRM

DRAFT

Appendix A – TIU Note with Vital Signs

The TIU note below shows what should be produced by the CFTV system. Note that the TIU note is produced in response to HL7 messages to the VistA TIU note package sent by the CFTV Interface Package.

Example 1 (with VS):

LOCAL TITLE: TRANSFUSION VERIFICATION (BTRF) NOTE
STANDARD TITLE: BLOOD BANKING TRANSFUSION NOTE
DICT DATE: MAR 26, 2014@16:29 ENTRY DATE: MAR 26, 2014@16:29:59
DICTATED BY: MANAGER, SYSTEM EXP COSIGNER:
URGENCY: STATUS: COMPLETED
SUBJECT: Unit Id: BC000000

PATIENT INFORMATION:

Patient Blood Type: O POS

ORDER INFORMATION:

Order Number: 0000000
Ordering Provider: BCEPROVIDER, ONE
Blood Product Components: RED BLOOD CELLS
Blood Product Transfusion Requirement:
Transfusion Priority: Routine
Donor Blood Type: O Neg
Unit Issued From Blood Bank Date/Time: Mar 26, 2014 16:06:27
Blood Product Unit Id: BC000000
Expiration Date: Apr 25, 2014 23:59:00

PRE TRANSFUSION INFORMATION:

Pre-Transfusion Checklist
: Verify patient consent Yes
: Verify Provider/Physician order Yes
: Premedication administered Yes
: Pt. educated r/t procedure/risks Yes
: Verify patent IV access Yes
Pre-Transfusion Comments: new comment here
Transfusion Documentation Workflow: Standard

TRANSFUSION INFORMATION:

Transfusionist ID #1: FIRST BCENURSE
Transfusionist ID #2: SECOND BCENURSE

Transfusion Begin Date/Time: Mar 25, 2014 16:27:49
Expired Override Reason: Blood Bank Authorized
Admin Set/Filter Type: Alaris Blood Tubing (Pump)
Admin Set/Filter Lot Number: 22

Transfusion Stopped Date/Time: Mar 25, 2014 16:28:18
Transfusion Stopped By User: FBCENURSE
Transfusion Stopped Reason(s): *Other Symptom
Stop Reason Comments: STOP TEST
Transfusion Stopped Action Taken: Blood Bank and Provider Notified
Stopped Volume (ml): 100
Transfusion Restarted Date/Time: Mar 25, 2014 16:29:10
Transfusion Restarted by User: FBCENURSE
Transfusion Completed Date/Time: Mar 25, 2014 16:29:54
Completed Volume (ml): 300
Completed By: FBCENURSE

VITAL SIGNS INFORMATION:

Vitals Taken: Mar 25, 2014 16:26:12
Entered By: FBCENURSE
Temp: 98.1
Pulse: 65
Resp: 20
Systolic BP: 160
Diastolic BP: 80
S/S Reaction: No
Vitals Taken: Mar 25, 2014 16:28:34
Entered By: FBCENURSE
Temp: 98.2
Pulse: 66
Resp: 21
Systolic BP: 160
Diastolic BP: 81
S/S Reaction: No
Vitals Taken: Mar 25, 2014 16:29:13
Entered By: FBCENURSE
Temp: 98.3
Pulse: 67
Resp: 75
Systolic BP: 160
Diastolic BP: 55
S/S Reaction: No

/es/ BCENURSE, FIRST
BCENURSE, FIRST
Signed: 03/26/2014 16:29

Appendix B – Acronyms and Definitions

Table 39 shows the acronyms and definitions used in this PD SDD.

Table 38: Acronyms and Definitions

Acronym	Definition
AABB	American Association of Blood Banks
ADT	Admission Discharge Transfer
AITC	Austin Information Technology Center
AP	Anatomic Pathology
BAPOC	Blood Administration Point of Contact
BCE-PPI	Bar Code Expansion – Positive Patient Identification
BCMA	Bar Code Medication Administration
BCRO	Bar Code Resource Office
BTRF	Blood Transfusion Record Form
CAB	Cabinet
CAP	College of American Pathologists
CCB	Change Control Board
CF	CareFusion
CFIE	CareFusion Interface Engine
CFMC	CareFusion Management Console
CFTV	CareFusion Transfusion Verification
CONOPS	Concepts of Operations
COOP	Continuity of Operations
COTS	commercial-off-the-shelf
CPE	Capacity and Performance Engineering
CPRS	Computerized Patient Record System
CPU	Central Processing Unit
CQ	ClearQuest
CR	Change Request
DBMS	Database Management System
DCO	Data Center Operations
DOB	Date of Birth
DR	Disaster Recovery
DRS	Distributed Resource Scheduler
EDA	Enterprise Digital Assistant
ESE	Enterprise Systems Engineering
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GUI	Graphical User Interface
HA	High – Availability
ICD	Interface Control Document
IIS	Internet Information Services
JDK	Java Development Kit
JSP	Java Server Pages

Acronym	Definition
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
MTP	Master Test Plan
MUMPS	Multi-User Multi-Programming System
NDC	National Data Center
NIST	National Institute Standards and Technology
NSR	New Service Request
OAP	Operational Acceptance Plan
CPRS	Computerized Patient Record System
OIT	Office Information Technology
OMB	Office of Management and Budget
OS	Operational System
PD	Product Development
PIA	Privacy Impact Assessment
PIMS	Patient Information Management System
PMAS	Project Management Accountability System
PMP	Project Management Plan
POC	Point of Contact
POM	Production Operations Manual
PPOC	Patient Point of Care
PROD	Production
RDC	Regional Data Center
RPC	Remote Procedure Call
RSD	Requirements Specification Document
RTM	Requirements Traceability Matrix
SCMP	Software Configuration Management Procedures
SCMPD	Software Configuration Management Procedures Document
SDD	System Design Document
SDLC	Software Development Life Cycle
SEDR	System Engineering Design Review
SLAM	Service Level Agreement Modification
SNMP	Simple Network Management Protocol
SQA	Software Quality Assurance
SUT	System-Under-Test
TBD	To Be Determined
TIU	Text Integration Utility
TJC	The Joint Commission
TRM	Technical Reference Model
TV	Transfusion Verification
VA	Veterans Affairs
VA	Veterans Administration
VAMC	Veterans Affairs Medical Center
VBECS	Veterans Blood Establishment Computer System
VDD	Version Description Document
VDL	VistA Document Library

Acronym	Definition
VistA	Veterans Integrated System of Technological Architecture
VLER	Virtual Lifetime Electronic Record
VM	Virtual Machine
WEP	Wired Equivalent Privacy
WIR	Wireless Infrastructure Replacement
WMA	Wireless Medication Administration
WPA	Wi-Fi Protected Access

Appendix C - Glossary of Terms

Table 40 shows the meaning for all terms used in this PD SDD.

Table 39: Glossary of Terms

Term	Meaning
ADT HL7	ADT messages carry patient demographic information for HL7 communications but also provide important information about trigger events (such as patient admit, discharge, transfer, registration, etc.). Some of the most important segments in the ADT message are the PID (Patient Identification) segment, the PV1 (Patient Visit) segment, and occasionally the IN1 (Insurance) segment. ADT messages are extremely common in HL7 processing and are among the most widely used of all message types.
Apache Tomcat	Open source software implementation of the Java Servlet and JavaServer Pages technologies
Authentication	A security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
bapiservice	Web service application that enables communication between Pyxis® Med Admin VA and Vista Vitals package via RPC architecture.
BCRO	The BCRO was established within the Veterans Health Administration (VHA) to provide centralized leadership and strategic direction for the use and implementation of bar code technology within critical health care systems at the enterprise level. The BCRO is the business sponsor for the Bar Code Expansion-Positive Patient Identification project.
Bar Code Expansion-Positive Patient Identification (BCE-PPI)	The goal of the Bar Code Expansion-Positive Patient Identification (BCE-PPI) project is to decrease patient misidentification and vulnerabilities in labeling of blood and laboratory specimens and to eliminate the need to use paper to record patient information before manually entering patient information in to the CPRS. BCE-PPI will deploy a set of applications to enhance patient care through wired and wireless communications facilitated by a set of software applications developed for that purpose. The applications will enhance the quality of care, improve quality control, and decrease the number of adverse events due to patient misidentification. BCE-PPI will accomplish this through the implementation of five commercial software applications, including WMA and documentation, electronic medical record browsing, nursing documentation of vital signs and additional monitoring data, specimen collection (both clinical lab and anatomic pathology) and labeling, and blood administration. These products will be used in conjunction with existing applications in VA such as the Veterans Health Information Systems and Technology Architecture (Vista), CPRS, BCMA, and HealtheVet.

Term	Meaning
CF	CareFusion – Trademarked product name for the suite of products provided by Medtech/CareFusion, the COTS vendor for the BCE-PPI project.
CF Interface Engine (CFIE)	The CareFusion Interface Engine (also known as the interface package) handles the translation and processing of HL7 messages used to exchanges data between the CFTV system, VBECS and VistA.
CF Management Console (CFMC)	Allows users to manage and configure settings of the CFTV application server.
COTS	Short for <i>commercial off-the-shelf</i> describes software or hardware products that are ready-made and available for sale to the general public.
CPRS	CPRS provides an integrated patient record system for clinicians, managers, quality assurance staff, and researchers. The primary goal of CPRS is to create a fast and easy-to-use product that gives physicians enough information through clinical reminders, results reporting, and expert system feedback to make better decisions regarding orders and treatment. VISTA software integrated with CPRS includes Pharmacy, Lab, Radiology, Allergy Tracking, Consults, Dietetics, Progress Notes, Problem List, Patient Administration, Vitals, PCE, TIU, ASU and Clinical Lexicon.
FIPS 140-2	Security requirements for Cryptographic Modules (FIPS PUB 140-2). This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information).
IEEE 802.11	Standard wireless local area network protocol.
Interface Control Document (ICD)	Interfaces are documented in Interface Control Documents (ICDs). ICDs are the formal means of establishing, defining, and controlling interfaces and for documenting detailed interface design definition for BCE-PPI. The ICD for BCE-PPI increment 2 is available on the BCE-PPI SharePoint site.
LAN protocol	There are several specifications within 802.11 (802.11a, 802.11b, 802.11g & 802.11i). The latest protocol provides improved security and bandwidth, access control and authentication for both wireless and wired networks.
Microsoft® Structured Query Language (SQL) Server 2008	Microsoft's Relational Database Management System (RDBMS). The current version is 2008 R2.
Microsoft® Windows Server 2008	Microsoft Windows' server operating system. Released to manufacturing on February 4, 2008, and officially released on February 27, 2008, it is the successor to Windows Server 2003, released nearly five years earlier. A second release, named Windows Server 2008 R2, was released to manufacturing on July 22, 2009. Windows Server 2008 is based on Windows NT 6.x.

Term	Meaning
MicroTech CF Commercial Off-The-Shelf (COTS) software	CF will provide the VA with a suite of positive patient identification products to help reduce the potential for errors during specimen collection and blood transfusion. The Pyxis® Specimen Collection Verification system focuses on ensuring clinicians correctly label and collect a patient's lab specimens and the Pyxis® Transfusion Verification system ensures the appropriate blood product is transfused to the right patient at the right time.
Motorola MC75AO EDA	Hardware-level wireless scanner, security compliant with the FIPS 140-2 policy in accordance with VA wireless security policy. The MC75AO is the only EDA device meeting VA TRM_0067OP-EDA requirements that is constructed of healthcare plastics.
NSR	Requests for business problem analysis potentially utilizing Information Technology (IT) as an enabler. NSRs are the Veterans Health Administration (VHA) users' tool to request IT support and solutions for the VHA information systems and are designed to address arising needs.
Office of Information and Technology (OIT)	<p>The Office of Information and Technology (OIT) is the steward of VA's IT assets and resources, and is responsible for ensuring the efficient and effective operation of VA's IT Management System to meet mission requirements of the Secretary, Under Secretaries, Assistant Secretaries, and other key officials.</p> <p>The office is composed of seven major organizational elements:</p> <ul style="list-style-type: none"> • <u>Oversight & Compliance</u> • <u>Quality & Performance</u> • <u>IT Information Security</u> • <u>Architecture, Strategy and Design</u> • <u>IT Resources Management</u> • <u>Product Development</u> • <u>Office of Service Delivery and Engineering.</u>
Oracle Java Virtual Machine (JVM)	Interprets compiled Java intermediate code (byte code) into executable (binary code) for specific computer hardware.
EDA	Generic term for a class of small easily carried electronic devices used to store and retrieve information.
Public Key Infrastructure (PKI)	Secure electronic mail using authentication and encryption with use of digital certificates. PKI is a credentials service; it associates user and entity identities with public keys.
Pyxis® Med Admin VA	Client GUI application used to bar code scan medication administered at the point of care
Pyxis® Nurse	Client GUI application that allows clinician to enter/edit patient at the point of

Term	Meaning
Assist VA	care.
Pyxis® Transfusion Verification	<p>Pyxis® TV is a barcode-enabled wireless application that helps hospitals significantly reduce the potential for errors during the blood transfusion process by promoting positive patient identification and positive blood product identification at the point of care.</p> <p>The system provides comprehensive transfusion safety at the bedside that helps ensure the correct patient receives the correct blood product.</p>
Pyxis® TVVA	Client GUI application that allows user to positively identify patients and document blood product infusion encounter.
Regional Data Center (RDC)	A VA data center hosting the (virtual) machines needed to provide services to a given region. A region is a large collection of VA medical delivery facilities, including VAMC's and outlying clinics.
Blood Transfusion Record Form	A form printed in the blood bank used to record the actual events of a transfusion.
SQL (Structured Query Language)	Structured Query Language is a special-purpose programming language designed for managing data in relational database management systems (RDBMS).
TIU	Text Integration Utilities (TIU) was developed to collect, organize, and present clinical documentation easily and quickly. Progress Notes, Discharge Summaries, and Consults are the main components included with TIU.
Transfusion (Blood Transfusion)	Process of receiving blood products into one's circulation intravenously.
VHA Directive 2006-069	RESCISSION OF <u>VHA DIRECTIVE 2006-069</u> , PURCHASING BAR CODE SCANNERS, WRISTBAND PRINTERS, AND WRISTBAND PRINT MEDIA FOR USE WITH BAR CODE CLINICAL APPLICATION SOFTWARE
VistA	<p>Veterans Health Information Systems and Technology Architecture (VistA) is the proprietary software developed for and used by Department of Veterans Affairs (VA) Veterans Health Administration (VHA) to support its clinical and administrative functions at VA sites nationwide. It is both client- and server-based software. The client-based software is written in Java, Borland Delphi Pascal, and other GUI-based languages and runs on the Microsoft operating system. The server-based software is written in the M programming language, and, via Kernel, runs on all major M implementations regardless of vendor.</p> <p>It is composed of integrated clinical, infrastructure, and financial/administrative software applications. This internally developed portfolio of applications is recognized as the most comprehensive integrated health information system in the U.S.</p>
Vista Blood Establishment	Vista Blood Establishment Computer Software (VBECS) automates the daily processing of blood inventory and patient transfusions in a hospital transfusion

Term	Meaning
Computer System (VBECS)	service. VBECS is an improved Blood Bank application that facilitates ongoing compliance with Food and Drug Administration (FDA) standards for medical devices and enhances the VA VHA's ability to produce high-quality blood products and services to veterans. The system follows blood bank standards, standards of national accrediting agencies, FDA regulations, and VA policies.
VistA Remote Procedure Call (RPC)	A remote procedure call (RPC) is an invocation of a subroutine on a remote system by code on a local system. In the VA case an RPC invokes a routine in the M language. The remote procedure called may take optional parameters to do some work and then return either a single value or an array back to the client application. RPC's are the standard method of communication between a Windows (clinical) client application such as CPRS and the VistA server. RPC's are also used to integrate COTS and GOTS systems with VistA.
WBCService	Web service application that enables communication between Pyxis® TVVA and VistA Vitals package via RPC architecture.
Wired Equivalent Privacy (WEP)	An algorithm, part of the 802.11 standard, which is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but is frequently considered to be a feature of WEP.
Wireless	Technology that permits the transfer of information (active or passive) between separated points without physical connection. Currently, wireless technologies use infrared (IR), acoustic, radio frequency (RF), and optical technology; but as technology evolves, wireless could include other methods of transmission. Active information transfer entails emanation of energy, whereas passive information transfer includes stand-alone storage devices that can record audio and video information.
Wireless Access Point	Network equipment that provides wireless connection to the network.
Wireless Workstation	A computer (laptop or desktop) which is connected to the internet using a wireless connection. In the context of CFTV it means a computer running the Pyxis desktop client application.
wswCareAssistVA	Web service application that enables communication between Pyxis® Nurse Assist VA and VistA Vitals package via RPC architecture.

Appendix D – References

Project documents for increment 2 are published in the BCE-PPI SharePoint repository. A link to the repository is provided here:

[http://\[REDACTED\]](http://[REDACTED])

Documents which do not contain proprietary material are published in the VistA Document Library (VDL).

[http://\[REDACTED\]](http://[REDACTED])

Links to access specific documents mentioned in the body of the SDD are provided below:

1. Project Management Plan (PMP)

[http://\[REDACTED\]](http://[REDACTED])

2. Requirements Specification Documents (RSD)

The requirements that the integrated design must meet are detailed in the RSD for increment 2, which is titled:

BCE-PPI Increment 2 VistA Applications / VBECS Interfacing with a COTS BAPOC System

[http://\[REDACTED\]](http://[REDACTED])

3. Test Evaluation Summary (TES)

[http://\[REDACTED\]](http://[REDACTED])

Important deliverables within the TES document include:

- Evaluation Summary and Recommendation
- Site Evaluation Log
- Site Evaluation Defect Log
- Site Evaluation Plan

4. Deployment Plan

[http://\[REDACTED\]](http://[REDACTED])

5. Product Operations Manual (POM)

[http://\[REDACTED\]](http://[REDACTED])

6. MJCF (VistA) Installation Guide,

[http://\[REDACTED\]](http://[REDACTED])

7. MJCF (VistA) Technical Manual

[http://\[REDACTED\]](http://[REDACTED])

8. CareFusion Transfusion Verification (CFTV) Installation Guide,

[http://\[REDACTED\]](http://[REDACTED])

9. EDA Device Configuration Manual

[http://\[REDACTED\]](http://[REDACTED])

10. Operations Acceptance Plan (OAP)

[http://\[REDACTED\]](http://[REDACTED])

11. SDE SDD for Increment 2

VA_Enterprise Systems Engineering (ESE)_BCE-PPI_DESIGN_vA.0.5.vsd

[http://\[REDACTED\]](http://[REDACTED])

13. CareFusion Client Manual for Handheld (EDA)

[http://\[REDACTED\]](http://[REDACTED])

14. CareFusion Client Manual for Desktop Client

[http://\[REDACTED\]](http://[REDACTED])

15. CareFusion Transfusion Verification Features

[http://\[REDACTED\]](http://[REDACTED])

16. VistA HL7 Documents (leading reference in the VistA Document Library)

[http://\[REDACTED\]](http://[REDACTED])

17. VistA Kernel

[http://\[REDACTED\]](http://[REDACTED])

18. VistA ADT:

[http://\[REDACTED\]](http://[REDACTED])

19. VBECS:

[http://\[REDACTED\]](http://[REDACTED])

Appendix E – Data Elements for the VBECS to CFTV Interfaces

This appendix describes interfaces IF9 and IF10, which are the inbound and outbound interfaces to the CFTV server. Both of these interfaces employ standard HL7 messages, but the messages have been modified slightly by the COTS vendor to fit the specific needs of the CareFusion CFTV system as deployed within the VA. We note that the handling of time and time zones in the HL7 messages for IF9 and IF10 is an ongoing concern. The workarounds used for time-stamping messages and dealing with situations in which the CFTV server is in a different time zone than the VBECS server are described in this section. In principle, the case in which the CFTV server is in a different time zone than the client applications needs to be addressed in this appendix as well. However, since this situation has been deliberately avoided in the deployment of BCE-PPI Increment II we will defer discussion. At present, additional CFTV servers have been added to the RFC's with their time zones set to match both their partner VBECS servers and their clients. This means that a time zone mismatch between the CFTV server and its VBECS partner cannot occur. The same applies to CFTV server/client mismatches.

CareFusion has taken the position that handling time zone mismatches without creating additional CFTV servers to match time zones is a system enhancement. When that enhancement is made we will update this document to provide details of timestamp and time zone handling by the enhanced CFTV Interface Package.

Pyxis® Transfusion Verification Interface Data Structures

As noted earlier, transfusion orders are sent to from the VBECS server to the CFTV servers HL7 BPS-029 messages. The CareFusion document cited below refers to this direction as 'inbound' since it is written from the viewpoint of the CFTV server. Blood product administration status messages are sent from the CFTV server to VBECS in the form of HL7 BTS-031 messages. The CareFusion document refers to this direction as "outbound."

Pyxis® Transfusion Verification Interface General Information

Abstract:

This document provides a detailed listing of the required messages and required data to be exchanged in order to support Pyxis® Point of Care Transfusion Verification application. Pyxis® Transfusion Verification is designed to assist the clinician with the transfusion of blood products. The interface engine supports Pyxis® Transfusion Verification by providing a real-time Gateway between Pyxis® and the Hospital Information System. Pyxis® Point of Care Verification exchanges messages with the Hospital Information System by using TCP/IP connections that support synchronous message exchanges. Upon receipt of a message, the interface engine sends an appropriate acknowledgement message to the Hospital Information System as described in the HL7 Version 2.5 specification.

Inbound to Pyxis® Point of Care Verification

The interface engine accepts incoming, unsolicited BPS messages for blood products that have been assigned to a patient for transfusion, dispositioned/relocated from the blood bank, and/or released back to inventory or waste. These messages are generated by the Hospital Information System and sent to the interface engine. In response to a BPS message, Pyxis® Point of Care Verification will reply with an ACK message to indicate the receipt of the HL7 message.

General Message Information

The interface engine can be customized to handle implementation specific message construction logic. However, the following implementation rules are suggested:

Each message should start with the UNICODE character represented by the hexadecimal value 0x0B which is equivalent to the character with a decimal value of 11.

Each message should end with the UNICODE character represented by the hexadecimal value 0x1C which is equivalent to the character with a decimal value of 28.

Each message segment should end with the UNICODE character represented by the hexadecimal value 0x0D which is equivalent to the character with a decimal value of 13.

Interface engine expects the suggested default component separator is a “|” per the HL7 2.5 specification. Interface engine also expects the suggested

encoding characters outlined in the HL7 specification, ^~\&ication ACK - AR

Due to the existing interfaces between Pyxis® and the VA, the ADT interface will follow the following character delimiters when implementing this ADT interface.

- All fields will be separated with a “^”
- All subfields will be separated with a “~”
- Repeating fields will utilize the “|”
- The encoding characters will be “~\&”

Transfusion Order Messages

This section provides a listing of the required messages that need to be exchanged in order to implement the Pyxis® Transfusion Verification application.

Key:

[] = HL7 Segment is Optional within this Sequence

{ } = HL7 Segment can Repeat within this Sequence

Event Type/ Trigger	Description	HL7 Segment Layout
BPS~O29	Blood Product Dispense Status Message (inbound)	MSH Message Header PID Patient Identification PV1 Patient Visit Information ORC Common Order Segment BPO Blood Product Order BPX Blood Product Dispense Status [{OBX}] Observation/Result Segment
BRP~O30	Blood Product Dispense Status Message Acknowledgement Message	MSH Message Header MSA

After receiving a **BPS** message, the Pyxis® Interface Engine sends an ACK message back with "**BRP~O30**" or "**BRP~O30**" in **MSH-8**.

Upon receipt of a new transfusion order, Pyxis® Point of Care Verification will query the database to determine if the patient exists. If the patient does not exist, PPOC will create the patient, as well as the order. If the patient already exists, PPOC will create the order to the patient's record

Inbound to Pyxis® Point of Care Verification

The interface engine accepts incoming, unsolicited BPS messages for blood products that have been assigned to a patient for transfusion, dispositioned/relocated from the blood bank, and/or released back to inventory or waste. These messages are generated by the Hospital Information System and sent to the interface engine. In response to a BPS message, Pyxis® Point of Care Verification will reply with an ACK message to indicate the receipt of the HL7 message.

The Inbound Pyxis® Transfusion Verification Order HL7 Message is described using the following Segment Mappings:

- MSH Segment Layout
- PID Segment Layout
- PV1 Segment Layout
- ORC Segment Layout
- BPO Segment Layout
- BPX Segment Layout
- Observation/Result Segment (OBX)

BPS Message MSH Segment Layout

The MSH segment is primarily used to define the intent, source, and destination of an HL7 message. This message segment is critical to the successful exchange of information.

The detailed field-level format of the segment appears on starting page 6 of the CareFusion Transfusion Verification Interface Document.

BPS Message PV1 Segment Layout

The PV1 message segment is used to exchange patient information that is associated with specific patient visits.

The detailed field-level format of the segment appears starting on page 13 of the CareFusion Transfusion Verification Interface Document.

BPS Message ORC Segment Layout

The ORC segment contains fields that are common to all types of orders and must be included in the transfusion order message.

The detailed field-level format of the segment appears starting on page 13 of the CareFusion Transfusion Verification Interface Document.

BPO Segment Layout

The BPO segment provides accompanying details regarding the blood product component, such as special processing requirements and the amount of blood product to be administered

The detailed field-level format of the segment appears starting on page 20 of the CareFusion Transfusion Verification Interface Document.

BPX Segment Layout

The BPX segment contains additional information regarding the blood products requested, such as the unique donation ID, product code, blood type, expiration date/time, and current status of the product.

The detailed field-level format of the segment appears starting on page 21 of the CareFusion Transfusion Verification Interface Document.

Observation/Result Segment (OBX)

The OBX segment is used to carry information related to a single observation. There may be multiple OBX segments within a single message.

The detailed field-level format of the segment appears starting on page 22 of the CareFusion Transfusion Verification Interface Document.

Outbound - From Pyxis® Point of Care Verification

As noted, the CFTV server sends Transfusion Verification Transfusing Status Messages (BTS~O31 Messages) to applications that interface with CareFusion.

Outbound Pyxis® Transfusion Verification HL7 Segment Mappings

The BTS-031 message is segmented. We describe the function of the segments below, in the following order:

MSH Segment Layout
PID Segment Layout
PV1 Segment Layout
ORC Segment Layout
BPO Segment Layout

BTX Segment Layout
NTE Segment Layout

MSH Segment Layout

The MSH segment is primarily used to define the intent, source, and destination of an HL7 message. This message segment is critical to the successful exchange of information between systems.

The detailed field-level format of the segment appears starting on page 26 of the CareFusion Transfusion Verification Interface Document.

PID Segment Layout

The PID message segment is used to exchange patient identification information that changes on an infrequent basis. The value used for the patient identifier is implementation specific and should be agreed upon by each parties respective interface engineers. By default, the Interface Engine by Pyxis® Point of Care Verification will utilize the Account Number valued in PID-18, as the patient's primary unique identifier.

The detailed field-level format of the segment appears starting on page 28 of the CareFusion Transfusion Verification Interface Document.

PV1 Segment Layout

The PV1 message segment is used to exchange patient information that is associated with specific patient visits.

The detailed field-level format of the segment appears starting on page 30 of the CareFusion Transfusion Verification Interface Document.

ORC Segment Layout

The ORC segment contains fields that are common to all types of orders and must be included in the order message.

The detailed field-level format of the segment appears starting on page 33 of the CareFusion Transfusion Verification Interface Document.

BPO Segment Layout

The BPO segment provides accompanying details regarding the blood product component, such as special processing requirements and the amount of blood product to be administered.

The detailed field-level format of the segment appears starting on page 34 of the CareFusion Transfusion Verification Interface Document.

BTX Segment Layout

The BTX segment provides information regarding the transfusion and/or disposition of a blood unit. Specific details are transmitted via this segment, such as the administered volume and the interruption reasons

The detailed field-level format of the segment appears starting on page 35 of the CareFusion Transfusion Verification Interface Document.

NTE Segment Layout

The NTE segment is used to transmit comments associated to the transfusion.

The detailed field-level format of the segment appears starting on page 35 of the CareFusion Transfusion Verification Interface Document.

Appendix F - Approval Signatures

This section is used to document the approval of the PD SDD during the Formal Review. The review should be ideally conducted face to face where signatures can be obtained 'live' during the review however the following forms of approval are acceptable:

1. Physical signatures obtained face to face or via fax
2. Digital signatures tied cryptographically to the signer
3. /es/ in the signature block provided that a separate digitally signed e-mail indicating the signer's approval is provided and kept with the document

The Chair of the governing Integrated Project Team (IPT), Business Sponsor, IT Program Manager, Project Manager, and the members of the Technical and Enterprise Architectural Review Team are required to sign. . Until the Engineering and Architecture Review Board is stood up, both the Engineering IPT member(s) and the Architecture IPT member(s) must approve/sign the PD SDD. Please annotate signature blocks accordingly.

Signed:

Date:

██████████, Project Manager, Bar Code Expansion-Positive Patient Identification (BCE-PPI)

Signed:

Date:

██████████, Director, BCRO