

**VA Enterprise Design Patterns
Mobility**

Mobile Veteran-Facing Applications

**OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)**

VERSION 1.0

DATE ISSUED: NOVEMBER 2015



CONTENTS

1	Introduction	4
1.1	Business Need	4
1.2	Approach	4
2	Current Capabilities and Limitations	5
3	Future Capabilities	6
3.1	Mobile Strategy for Veteran-Facing Applications	6
3.2	User Experience.....	7
3.3	Type of Applications.....	8
3.4	Centralized Application Store.....	9
3.5	Scalable and Secure Infrastructure	9
3.6	Analytics and Metrics.....	10
4	Use Cases	10
4.1	Use Case #1	10
4.2	Use Case #2	13
	Appendix A. Scope	15
	Appendix B. Definitions.....	17
	Appendix C. Acronyms	18
	Appendix D. References, Standards, and Policies.....	20
	Table 1: Current Set of Veteran-Facing Applications.....	5
	Table 2: Use Cases.....	10
	Figure 1: Phased Roadmap to address Current Limitations	6
	Figure 2: Use Case #1 - Veteran Updates Address	12
	Figure 3: Use Case #2 - Veteran Accesses Data Across Lines of Business	14

1 INTRODUCTION

Secretary Robert A. MacDonald observed in his 2014 MyVA Presentation that “Assessments informing the [2014-2020] strategic plan told us VA often provides a fragmented, disjointed experience that result in poor customer service and frustrated Veterans and beneficiaries.” The Secretary described how Veterans and their beneficiaries take on the burden of serving as their own integration point for “multiple VAs.” Extending VA’s enterprise resources to an increasingly technology-savvy and mobile Veteran population is a high priority for achieving strategic goals stemming from the MyVA initiative.

The purpose of this Enterprise Design Pattern is to establish an enterprise direction for Veteran-facing mobile computing using enterprise services and common Information Technology (IT) infrastructure platforms. This document focuses on technical capabilities supporting the “external user” component of the Mobile Architecture Design Pattern (see Appendix A). This document provides guidance on the use of a standardized mobile solution via an enterprise-wide mobile middleware platform capable of supporting a robust, Veteran-centric customer experience.

1.1 Business Need

Veteran-facing mobile applications will help VA close the “mobile” infrastructure gap outlined in the Enterprise Technology Strategic Plan (ETSP) and move the VA towards a future-state IT vision supporting all VA lines of business. Extending enterprise resources to mobile devices requires consistent visibility of Veteran data and a central location to update this information. Veterans require a single access point to review their data and update personal information. A single access point reduces the burden on VA employees who are manually assisting and updating information for Veterans.

1.2 Approach

Achieving a robust mobile infrastructure requires a multi-year initiative supported by Office of Information & Technology (OI&T) and Administration leadership that encompasses strategy, governance, and technology investments. Simply migrating the current commercial off-the-shelf (COTS) mobile middleware platform to a new platform is insufficient for resolving the current capability limitations discussed in Section 2. Section 3 includes a phased approach to establishing future-state capabilities based on industry best practices for public-facing applications.

2 CURRENT CAPABILITIES AND LIMITATIONS

The following figure presents the current set of applications Veterans can download from public application stores. These applications include both native (e.g., iOS, Android) mobile applications and HTML5-based mobile websites. These applications require validated external user credentials, including DoD Self-Service Logon (DS Logon), for accessing enterprise data.

TABLE 1: CURRENT SET OF VETERAN-FACING APPLICATIONS

Requires DoD Self Service Logon Account to log in	<u>14 Mobile Applications are available on the Public App Store, 10 of these are available on iOS only</u>		
Launchpad (Web App)	ACT Coach (iOS)	Mindfulness Coach (iOS)	PTSD Coach (iOS, Android)
Airborne Hazards & Open Burn Pit Registry (Web App)	CBT-I Coach (iOS)	Moving Forward (iOS)	StayQuit Coach (iOS)
Mobile Blue Button (Web App)	Concussion Coach (iOS)	Parenting2Go (iOS)	311 Vet (iOS, Android)
Summary of Care (Web App)	CPT Coach (iOS)	PE Coach (iOS, Android)	Move! Coach (iOS)
Veteran Appointment Request (Web App)	Exposure Ed (iOS)	PFA Mobile (iOS, Android)	

These applications provide a wide range of functionality to Veterans, however, the current architecture and runtime environments limit this mobile experience supporting the MyVA initiative. The limitations are as follows:

- Inconsistent Single Sign-On: Currently, five Veteran-facing applications provide access to electronic health records (EHRs). While the Launchpad application is intended to provide a Veteran access to applications requiring access to EHRs, gaining access to MyHealthVet and eBenefits from this portal requires a secondary login.
- Limited User Experience: Applications are developed to address business requirements with general assumptions about user interests. Applications are not shared with Veterans for feedback until late in the development process, or after launch.

- Lack of Multi-Platform availability: Over 50 percent of applications are iOS only, limiting the availability to Veterans with phones using other operating systems.
- Lack of scalable infrastructure: Current systems can only support 3,500 concurrent Veteran log-ins.
- Limited User Analytics: Analytics are only available for iOS Applications.
- Non-standard Veteran-Facing Application Maintenance: Applications have a three-month support period after which they become the responsibility of the business owner. There is no operations and maintenance support of applications beyond three months.
- Lengthy Compliance Reviews: The complexity of systems and the lack of a comprehensive testing capability, impact the current compliance turn-around times. Applications currently spend a minimum 33 percent of the development cycle in compliance review.

3 FUTURE CAPABILITIES

The phased approach to achieve future-state mobile capabilities to address limitations in Section 2 is as follows:



FIGURE 1: PHASED ROADMAP TO ADDRESS CURRENT LIMITATIONS

3.1 Mobile Strategy for Veteran-Facing Applications

The initial phase focuses on establishing an enterprise mobile strategy addressing technology, governance, compliance and security, and support as shown in Figure 1. VA is currently deploying Enterprise Shared Services (ESS) to support Veteran-facing applications, and VA will expand on them in the next three years. These services include support for standardized authentication and authorization (A&A) and scalable, enterprise-wide mobile middleware to support automated development and operations (DevOps), standardized analytics, and an enhanced mobile application store (Phases 2 and 3). Mobile middleware provided as an ESS supports the strategy through the following actions:

(Near-Term):

- ESS are established within the enterprise IT Infrastructure and are available to all approved applications and devices for authenticated users. Requires the appropriate authorizations for access.

(Mid-Term):

- Continued prioritization and execution of enhancements to old applications. Ensure capability of new applications to use ESS, as shown in the use case in Section 4.
- Enhance Identity and Access Management (IAM) for external users to ensure secure A&A provided as an ESS. Continue enhancing legacy applications and ensure capability of new applications to use ESS for A&A.

(End-State):

- Device-agnostic application development using HTML5 integrated with ESS.
- Enterprise compliance with procedures and policy for management of VA IT organizational processes including Risk Management, Change Management, and Disaster Recovery.
- All applications leverage centrally managed IT controls for mobile acquisitions of hardware, software and infrastructure integrated with A&A ESS.

The following subsections provide context for the requirements that future-state technical capabilities satisfy to resolve the Veteran-facing application limitations in Section 2.

3.2 User Experience

User experience is the process of enhancing the usability, accessibility, and interaction between the Veteran and the application. User experience comprises information architecture and visual design, and VA's requirements for Veteran-facing applications are as follows:

- Establish Focus Groups: Divide the Veteran population into focus groups. Generate a unique persona from each focus group. Build use cases on the personas and define how the system needs to act.
- Define a Service Request Capability: A Veteran issues a "service request" for the requested information. A service request for information is made to the existing database and presented to the Veteran.
- Design logical Information Architecture: Prioritize main features and contents on the landing page according to the Veteran's needs. Enable Veterans to navigate to the most important content and functionality in as few steps as possible.
- Leverage Device Capability: Use device features and capabilities to support the Veteran's context of use. Accommodate for changes in context depending on time of the day and when the Veteran is using the application. Use location to identify where the Veteran is and display relevant content.
- Provide Offline Data Access: An enterprise mobile app needs to support offline data access and maintain data integrity. Applications should have an encrypted database for short-lived data inside the app. This approach will address security concerns due to data at rest while providing vital information to a Veteran when offline.
- Enable Always-On Virtual Private Network (VPN): A Veteran currently enters credentials as many as three times to access data and again submits credentials when switching networks or whenever the phone goes into a sleep mode. The security of an Always-On VPN improves user experience without compromising security.

3.3 Type of Applications

Services will be consolidated so that Veterans have one interface to access and acquire the status of services and capabilities. A Veteran will be able to access information when offline (e.g., appointments). Applications will provide a temporary cache to store any updates as a Veteran moves between networks or is temporarily without network coverage. Uninterrupted access to relevant data improves customer experience. Veteran-facing applications use a mobile platform with one code base to support multiple operating systems (i.e., IOS, Android, Windows, etc.) and devices.

- Informational Applications: All informational applications need to be web applications. HTML5 based applications are device agnostic and provide cross platform support.
- Transactional Application: Consolidated services will provide Veterans one main application to transact and retrieve status on services and capabilities available to them. A native application with the ability to temporarily cache data delivers an increased user experience.

3.4 Centralized Application Store

A centralized application store will allow VA to more securely manage and distribute Veteran-facing applications to Veteran's devices from a central location ensuring:

- Mobile application discovery and distribution
- Multiple Platform Support
- User authentication for application installation
- Over-the-Air application installation, configuration, and updates
- Over-the-Air application removal for Veterans' devices
- End to end application management

3.5 Scalable and Secure Infrastructure

Veteran-facing applications require the following mobile infrastructure requirements to support the business needs:

- Deploy Mobile Middleware: Implement Scalable Mobile middleware by leveraging backend Service-oriented Architecture (SOA) services and security capabilities. An enterprise mobile middleware platform will support increased user availability.
- Adopt Single Sign-On: A Federated identity management system and a transition to IAM Single Sign-On (AccessVA) will facilitate the sharing of identity information across administrative boundaries. A Veteran will be able to login with a single set of credential to access the authorized services provided they have the right level of assurance.
- Establish Mobile Application Management: Veterans will be able to access ESS and data through their mobile applications. Mobile Application Management ensures application security and remote application management.
- Enforce Multi-Device and Multi-Channel Support: Veteran's applications work on any device, instantly and seamlessly. This multi-channel approach provides users access to available information, with a consistent user experience. Transitioning to cross-platform

development tools and an integration infrastructure will support a multichannel environment

3.6 Analytics and Metrics

Veteran-facing applications require the following analytics to support business needs:

- Define Metrics: Identify application performance metrics and usage metrics to demonstrate application adoption. Track application performance across multiple devices and device versions. Data providing metrics on slow web service calls, network performance, and service request performance will provide the information to evaluate the capacity of the infrastructure to support an increasing user base.
- Create Standardized Analytics: A standardized platform will allow Veteran usage data to be assessed over a variety of parameters. This platform will provide a single view of application usage that will help understand Veteran data access patterns.

4 USE CASES

The Veteran-facing application use cases demonstrate how a Veteran’s application will support ESS in accordance with the VA Enterprise Technical Architecture.

TABLE 2: USE CASES

Use Case	Use	Data Sensitivity
Veteran accesses, creates, or modifies personal non-public data	Veteran/caregiver accessing medical and patient data using a mobile device for medication and related care information, preventative care. This could also be a Veteran accessing Chapter 33 or other non-health benefits; Right information at the right time for the proper care.	VA Sensitive Data (SPI)/Personal Health Information (PHI) Administratively Confidential Information (ACI) (aka. PGD/IAM–DS/Logon/SSOe/OAuth)

4.1 Use Case #1

User Experience: Veteran makes a single change securely that is updated across all VA systems.

- A Veteran initiates a change of address through a mobile application to reflect the Veteran’s move from the Washington, DC area to the San Francisco, CA area.

- The Veteran can login using existing credentials established on VA systems or using an external approved Credential Service Provider (CSP).
- Veteran's token is validated and the CSP brokers the connection between the Veteran and the application.
- In the brokered connection, user information is passed to single sign on external (SSOe) integrated applications in HTTP headers, called SSOe Tokens.
- A data message is sent from the application through authoritative information services down to the data layer.
- The message is processed by the Enterprise Create, Read, Update, Delete (eCRUD) service, which writes the address change to the data lake and also to the ADS for Veteran addresses.

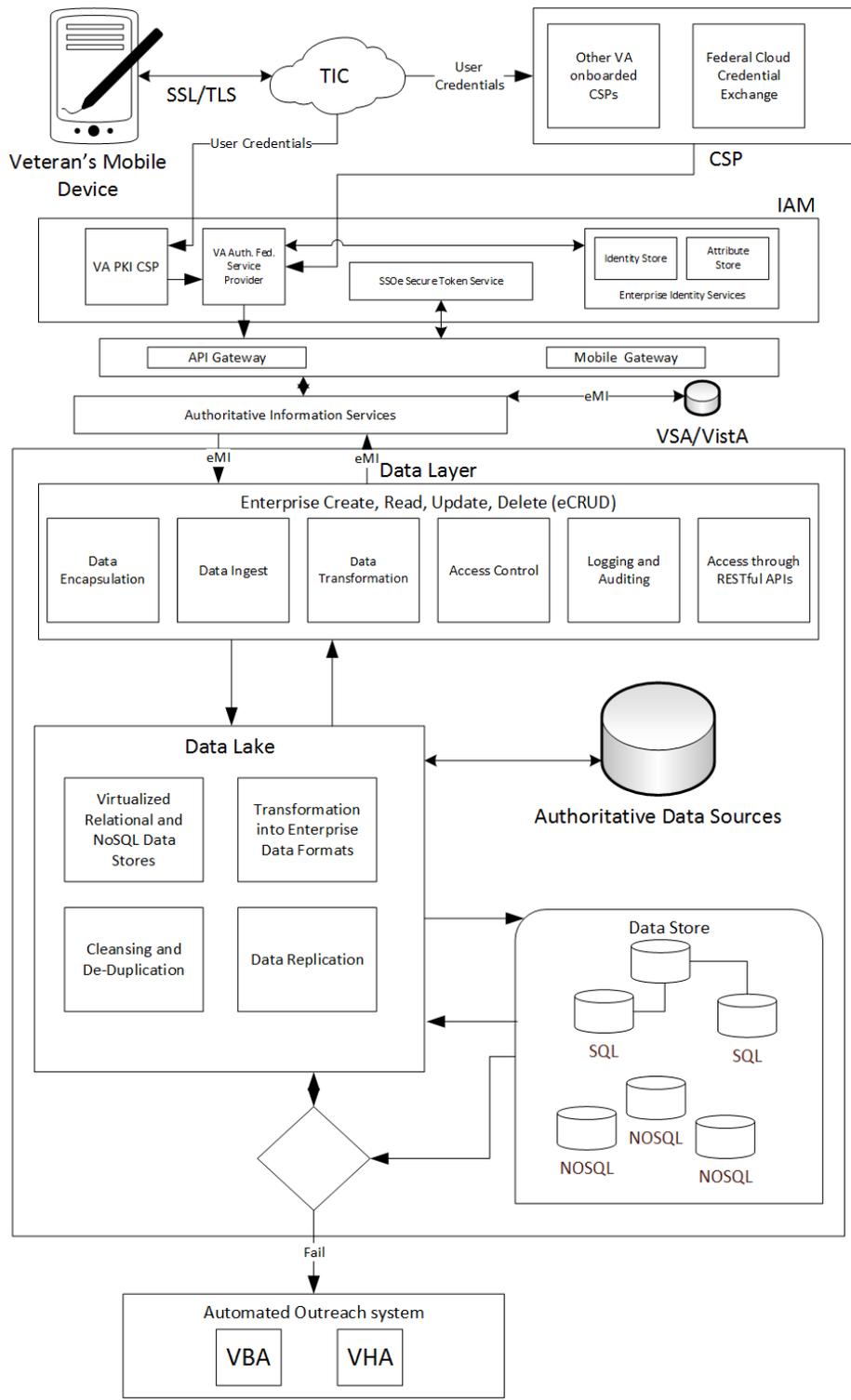


FIGURE 2: USE CASE #1 - VETERAN UPDATES ADDRESS

4.2 Use Case #2

User Experience: Veteran accesses a single application to access critical information pertinent to the Veteran. Veteran securely logs on using credentials previously established on an existing VA system.

- A Veteran accesses his or her medical prescription and then looks for benefits information through a mobile application.
- The Veteran can login using existing credentials established on VA systems or using an external approved Credential Service Provider.
- Veteran's token is validated and the CSP brokers the connection between the Veteran and the application.
- In the brokered connection, user information is passed to SSOe integrated applications in HTTP headers, called SSOe Tokens.
- Veteran selects option to view list of his or her prescriptions. Application calls on authoritative information services to access VistA for prescription records associated with Veteran's Veteran Health Administration (VHA) patient Identification (ID). Veteran can now view the information.
- Veteran now selects an option to view current benefits. Application calls on shared services to retrieve Veteran's benefit information. Information is displayed on the mobile device.

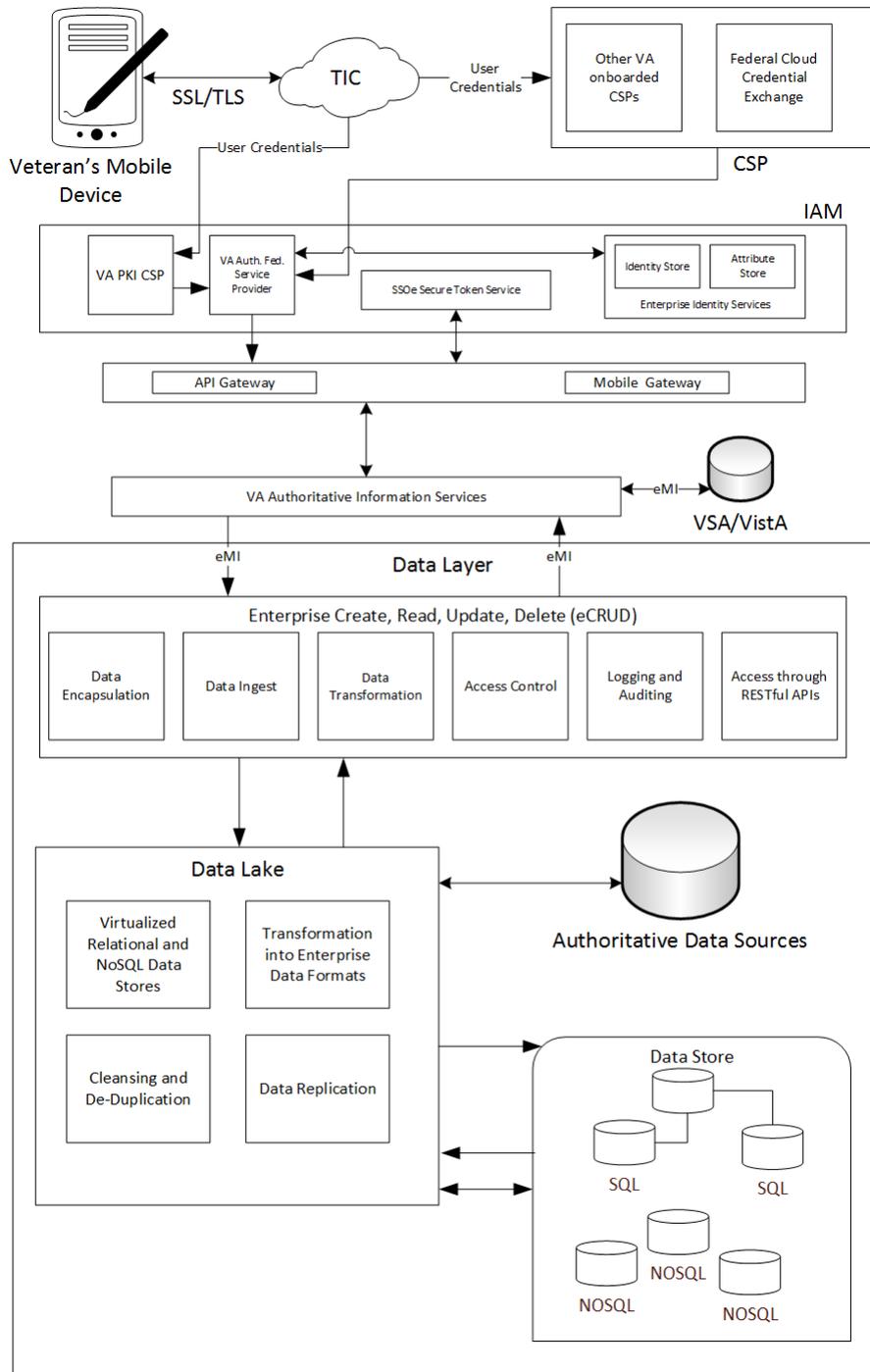


FIGURE 3: USE CASE #2 - VETERAN ACCESSES DATA ACROSS LINES OF BUSINESS

APPENDIX A. SCOPE

Scope

This Enterprise Design Pattern document provides an enterprise-level view of the current and future mobile capabilities relevant to Veteran-facing mobile applications and the standard processes in use. The document will refer to, rather than duplicate, lower-level solution guidance associated with these capabilities.

This document focuses on:

- A set of use cases that will allow Veterans to have access to VA services and their personal data through a single point of access or mobile gateway (i.e., VAMF).
- Veteran-facing mobile applications that are device agnostic, and will be able to perform on a wide variety of mobile devices that are commonly used by Veterans.
- What application development and deployment capabilities and constraints will need to be considered to provide application access to available ESS.
- Guidance that ensures a framework for seamless, Veteran-facing, user experience applicable to both internal VA mobile application development and 3rd party mobile application developers.

This Enterprise Design Pattern represents the external, Veteran-facing component of the overarching Mobile Architecture Design Pattern. The Enterprise Design Pattern document is generally applicable across all VA Lines of Business (LOB) and describes:

- Current VA mobile capabilities
- VA mobile infrastructure
- Processes to be used by the developers and the Veteran
- Enterprise-level mobile constraints, strategic guidance, and terminology

This Enterprise Design Pattern document **does not** address detailed technical solution guidance for implementing specific mobile applications. It will only provide the constraints to drive VA projects towards development of mobile solutions that effectively meet the specific goals of their initiatives.

- Topics that are out of scope for this Enterprise Design Pattern, but may be referenced, are:
- Mobile applications used by doctors, clinicians, and care-givers
- Mobile applications used by VA staff

- Interactions between wearable devices that produce patient generated data
- Certification processes for fielding applications
- Mobile security, including SSO

Intended Audience

The document is applicable to all programs and key stakeholders involved in developing and supporting mobile applications for Veterans across VA.

Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from VA's Office of Information and Technology (OI&T), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from VHA, Veteran Benefits Association (VBA), and National Cemetery Administration (NCA). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Enterprise Shared Service	A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions.
Service	A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description.
Service Oriented Architecture	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.

APPENDIX C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
AA&A	Authentication, Authorization and Audit
ACI	Administratively Confidential Information
ASD	Architecture, Strategy and Design
ADS	Authoritative Data Sources
ATO	Authority to Operate
BPE	Business Partner Extranet
COTS	Commercial Off the Shelf
EA	Enterprise Architecture
EAA	Enterprise Application Architecture
EHR	Electronic Health Record
eMI	Enterprise Messaging Infrastructure
EMM	Enterprise Mobility Management
ESCCB	Enterprise Security Change Control Board
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
ETSP	Enterprise Technology Strategic Plan
FHIR	Fast Healthcare Interoperability Resource
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
GFE	Government Furnished Equipment
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
IPT	Integrated Project Team
IT	Information Technology
LOB	Line of Business
MA	Mobile Application
MADP	Mobile Application Development Platform
MAGB	Mobile Application Governance Board
MAE	Mobile Application Environment
MAM	Mobile Application Management
MAP	Mobile Application Program
MARA	Mobile Application Reference Architecture
MAS	Mobile Application Store
MDM	Mobile Device Management
MHED	Mobile Health External Development
MVI	Master Veteran Index
NCA	National Cemetery Administration

Acronym	Description
NSOC	Network Security Operations Center
OIS	Office of Information Security
OI&T	Office of Information and Technology
OEF	Operation Enduring Freedom
PGD	Patient Generated Data
PHI	Protected Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PMAS	Project Management Accountability System
SAML	Security Assertion Markup Language
SDD	System Design Document
SDE	Service Delivery and Engineering
SDLC	Software Development Lifecycle
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SPI	Sensitive Personal Information
SSO	Single Sign-On – SSOe/SSOi: External and Internal designations
TIC	Trusted Internet Connection
TRM	Technical Reference Model
VAMF	VA Mobile Framework
VBA	Veteran Benefits Association
VHA	Veteran Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VLER	Virtual Lifetime Electronic Record
VPN	Virtual Private Network

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA Enterprise Technical Architecture (ETA):

#	Issuing Agency	Applicable Reference/Standard	Purpose
1	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in the VA, which applies to all applications that leverage ESS. http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=56
2	CIO Council	Government Mobile and Wireless Security Baseline	This document explains the essential elements of mobile computing (devices, access networks, agency infrastructure), and describes threats and risks to mobile computing.
4	CIO Council	Mobile Security Reference Architecture (MSRA)	The MSRA has been released by the Federal CIO Council and the Department of Homeland Security (DHS) to assist Federal Departments and Agencies (D/As) in the secure implementation of mobile solutions through their enterprise architectures.
5	VA MAP	VA Mobile Framework System Design Document	The VA Mobile Framework (VAMF) provides the infrastructure to allow VA Apps to be hosted in a standard architectural framework. It provides software services, including authentication of users and retrieval and updating of data within VA.

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the

content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.