VA Enterprise Design Patterns:

Mobility

Impact of Internet of Things (IoT)

Office of Technology Strategies (TS)
Architecture, Strategy, and Design (ASD)
Office of Information and Technology (OI&T)

Version 1.0

Date Issued: November 2016

THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

Gary E. Marshall 137891

Digitally signed by Gary E. Marshall 137891
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=gary.marshall@va.gov, cn=Gary E. Marshall 137891
Date: 2016.12.14 10:29:45 -05'00'

Gary Marshall
Director, Technology Strategies, ASD

PAUL A. TIBBITS 116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=paul.tibbits@va.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2017.02.01 09:59:36 -05'00'

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Organization	Notes
0.1	6/15/2016	ASD TS	Initial Draft/Outline
0.3	7/14/2016	ASD TS	Added content to Section 3
0.5	8/4/2016	ASD TS	• Revised previous content • Added content to Section 3 • Added use cases
0.7	10/11/2016	ASD TS	Incorporated stakeholder input from during and after the Public Forum
1.0		ASD TS	

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	7/6/2016	Nicholas Bogden	Enterprise Design Pattern Lead
0.3	8/4/2016	Nicholas Bogden	Enterprise Design Pattern Lead
0.5	9/28/2016	Nicholas Bogden	Enterprise Design Pattern Lead
0.7	11/15/2016	Nicholas Bogden	Enterprise Design Pattern Lead

TABLE OF CONTENTS

FIGURES

TABLES

1 INTRODUCTION

Emerging Internet of Things (IoT) technologies offer organizations opportunities to enhance their analytics and service delivery capabilities. IoT technologies pose security and asset management risks and challenges. This Enterprise Design Pattern (EDP) describes capabilities for mitigating the risks and maximizing the benefits of IoT technologies.

Examples of "things" in IoT include:

- Embedded systems
- Sensors, with or without actuators
- Fitness trackers[1]
- "Smart" objects and appliances

These examples are also known as IoT endpoints or endpoint devices. They are connected to a network via common Internet protocols, through some type of gateway (e.g., router, smartphone, or laptop). Endpoints are at the edge of a larger IoT solution that includes an IoT platform and back-end systems. Endpoints serve as data sources for analytics processes. They may or may not also initiate some action based on the output of those processes.

1.1 BUSINESS PROBLEM

The problems associated with IoT are not unique to the Department of Veterans Affairs (VA). IoT represents the latest iteration of networked embedded systems, and they encounter many of the same issues (particularly with regard to security) as well as some new ones. There are few established standards or best practices for mitigating inherent IoT security risks. These risks include:

1. **Poor endpoint device security**: Most devices are not patched to address known vulnerabilities, nor do they support being configured to meet VA security requirements.
2. **Difficulty of asset management:** Tracking large numbers of mobile endpoint devices is very difficult, especially for devices deployed beyond the organizational boundary.
3. **Distributed responsibility model:** Enterprise IoT managers must rely on device end users or vendors for some aspects of device operation and management.

[1] While fitness trackers may be used in a healthcare or health management context, they do not meet VA's definition of medical devices.

4. **Emerging and rapidly evolving technology:** Organizational policies and business units must be adaptable to IoT's rapid lifecycles and frequent changes.

1.2 BUSINESS NEED

The problems described in the previous section require an enterprise approach that will:

- Mitigate or avoid common IoT endpoint risks to both the devices themselves and the networks to which they are connected.
- Track and maintain IoT hardware assets that may be mobile, difficult to access, or in the hands of external end users beyond the organizational boundary.
- Articulate responsibilities and establish lines of communication between different roles involved in an IoT solution, including vendors, service providers, and end users.
- Establish processes for evaluating new IoT technologies and sharing data from existing deployed IoT solutions (as appropriate).

1.3 BUSINESS CASE

Despite significant risks, IoT offers numerous benefits. Table 1 lists some of the principal benefits VA can derive from using IoT solutions.

Table 1: Business Benefits

Business Benefits	Description
Real-time analytics and alerts[2]	• Provide valuable health data to clinicians and patients in a care management context • Enable rapid detection and rectification of facility/maintenance issues
Automation and responsive systems	• Reduce need for VA staff to perform manual data entry and reporting • Enable adaptive systems that automatically respond to environmental changes

[2] This capability aligns with VA's strategic goals as described in the Enterprise Data Analytics EDP.

Business Benefits	Description
Collect previously unavailable high-value data	• Obtain data previously available only through self-reporting • Extend data collection beyond VA's organizational boundary[3]

A comprehensive enterprise IoT program will enable VA to leverage the benefits of IoT while minimizing both inherent IoT risks, incidences of redundancy, and cost overruns.

1.4 APPROACH

This EDP describes a set of interrelated capabilities for a VA enterprise program to deploy and manage non-medical IoT solutions.[4] The proposed capabilities are informed by findings, recommendations, and best practices from VA's medical cybersecurity domain. They also draw on recommendations from the National Institute of Standards and Technology (NIST) related to Industrial Control Systems (ICS). The proposed capabilities consist of:

- IoT device security and risk management controls:
  - Baseline requirements for technology review, approval, and configuration of non-medical IoT devices.
  - Dedicated, isolated network segments for IoT devices, which can be deployed and configured in a standardized, repeatable, and scalable way.
- Comprehensive asset management for IoT endpoints, using an enterprise-wide IoT asset management system for:
  - Basic identifying information, including device type (e.g., medical, non-medical)
  - Device operational status
  - Configuration, version, and patch information
  - Performance and diagnostic data
  - Ownership by programs, facilities, and end users
  - Associated vendors and third-party IoT Platform Service Providers (IoTPSP)
- Established responsibilities and lines of communication for roles involved in IoT solutions, to include:

[3] With due attention and adherence to privacy, confidentiality, and consent requirements.
[4] Medical IoT devices will be addressed in a future Enterprise Design Pattern, and are out of scope for this document (see Appendix A).

    - VA enterprise IoT manager
    - Programs, projects, or Lines of Business (LOB) operating the device
    - Local VA facilities and technicians
    - Device vendors and service providers
    - Device end users
- Enterprise IoT help desk to assist projects in selecting new devices or using data from existing devices (as appropriate).

The proposed framework is sufficiently flexible to support a wide variety of IoT use cases and allow VA to adapt to the rapidly evolving field of IoT technologies. At the same time, the framework provides a consistent approach to addressing the security and asset management challenges presented by IoT endpoint devices.

A foundational concept of this EDP is the basic architecture common to all IoT solutions, regardless of vendor, use case, or underlying technology. This architecture consists of four parts, as shown in Figure 1:

- **IoT Endpoints:** The IoT "things" or devices themselves, such as sensors that collect data, indicators, or actuators that perform some action in response to commands.
- **Field Gateways:**[5] The aggregators that allow IoT devices to connect to the network. Gateways may include mobile devices (such as smartphones) or routers.
- **IoT Platform:** Service that provides data ingestion and device management for IoT endpoints, and may also refine/sequence ingested data.
- **Enterprise Backend:** Back-end VA applications and services that ultimately consume IoT data, and may issue commands to IoT devices.

[5] This component is called a "Field Gateway" to distinguish it from service-side gateways that provide and mediate connections to IoT platforms.

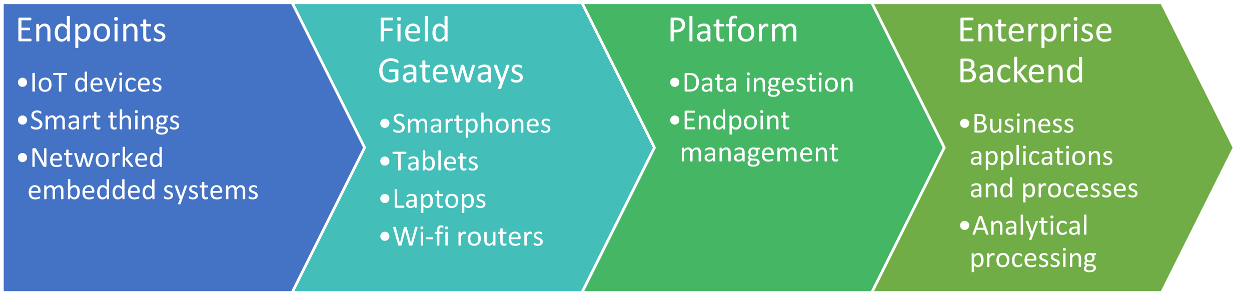

Figure 1: Illustration of a Four-Part IoT Solution Architecture

The Enterprise Backend component also issues commands to the IoT endpoints based on the results of analytics processes.

As IoT endpoints are effectively data collectors for analytic processes, IoT and analytics are inextricably linked. This EDP references concepts from the Enterprise Data Analytics EDP, to include data temperature and the five stages of an analytic dataflow. The five stages are illustrated in Figure 2:

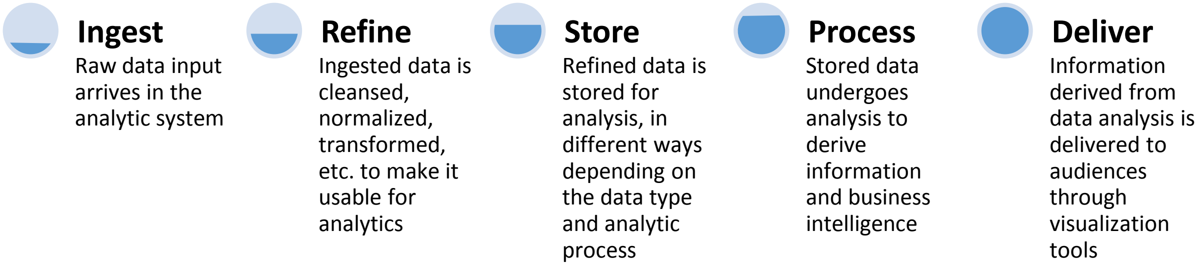
Ingest
Raw data input arrives in the analytic system
Refine
Ingested data is cleansed, normalized, transformed, etc. to make it usable for analytics
Store
Refined data is stored for analysis, in different ways depending on the data type and analytic process
Process
Stored data undergoes analysis to derive information and business intelligence
Deliver
Information derived from data analysis is delivered to audiences through visualization tools

Figure 2: The Five Stages of an Analytic Data Flow

In most IoT (though not all) solutions, the IoT Platform and Enterprise Backend components of the solution carry most of the analytic processing workload. The Endpoints or Field Gateways[6] may play a part in the Delivery stage (for example, if the Field Gateway in the IoT solution is a smartphone). This EDP assumes that the bulk of analytic processing workloads will be performed in the Platform and Enterprise Backend components.

[6] If the Field Gateway in the IoT solution is a smartphone, tablet, or laptop rather than a router, it can be used to support information delivery.

In some solutions, a certain degree of analytic processing may be performed in the Endpoint and Gateway components to trigger time-sensitive actions. This is appropriate and even necessary in certain use cases (i.e., triggering an emergency shutoff in response to environmental conditions), but may also introduce security risks. IoT solution architects are advised to keep the analytic processing workload in the Platform and Enterprise Backend components of a solution unless it is otherwise necessary.

It is important to note that this is still a target architecture at this time. VA has much of the Enterprise Backend components in place, but will need to acquire and deploy the other components to support IoT solutions.

2 CURRENT CAPABILITIES

VA does not currently have an enterprise-wide capability for managing IoT devices and solutions. While the Department has a number of sensored facility management systems (particularly in medical centers), these systems are not networked.

VA does, however, have a program for managing and securing network-connected medical devices. It also has an enterprise analytics capability that may be scaled out to accommodate IoT solutions.

2.1 MEDICAL DEVICE PROTECTION PROGRAM (MDPP)

VA established The Medical Device Protection Program (MDPP) to operate within a complex security landscape to apply cyber security and physical security principles to medical technology. The program is a collaborative effort between the VA Office of Information Security (OIS) Field Security Service (FSS) Health Information Security Division (HISD) and Veterans Health Administration (VHA) Healthcare Technology Management (HTM). The purpose of MDPP is to proactively manage risk associated with computer-based, network-connected medical devices.[7]

[7] As defined by HTM. Refer to Updated Security Requirements for Network Connected Medical Devices and Systems (VAIQ #7566605) at https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/Health%20Information%20Security%20Division/Memo%20-%20Security%20Requirements%20for%20Network%20Connected%20Medical%20Devices%20Feb%2013%20-%202015.pdf

One of the signature security controls of MDPP is the Medical Device Isolation Architecture (MDIA). An MDIA is a dedicated Virtual Local Area Network (VLAN), configured with an Access Control List (ACL). The MDIA ACL is used to strictly limit endpoint devices' external access to other devices, systems, and IT resources.

Another important aspect of MDPP is maintaining an inventory of network-connected medical devices. Under MDPP, VHA HTM is the authoritative source for:

- Defining what constitutes a medical device.
- Maintaining the official categorization and labeling of medical devices owned and operated by VA.
- The comprehensive list of medical device systems, using the VA Medical Device Nomenclature System (VA-MDNS).

VHA facility directors are responsible for keeping an accurate inventory of devices in their facilities and reporting that inventory to MDPP at specified intervals. MDPP captures and records all submitted inventory data at least once every 90 days.

Isolating IoT endpoints in their own dedicated network segment and maintaining a complete inventory of those devices are both best practices for IoT security and asset management. However, VA's Enterprise Cyber Security Strategy Team (ECST) has documented deficiencies in the current implementation of both MDIAs and medical device inventories.

The underlying hardware of MDIAs consists of network switches, which lack adequate memory, security features, and functionality to consistently fulfill security requirements. The current approach to configuring and maintaining MDIAs is largely manual, extremely burdensome, and prone to error. It also scales poorly, to the point where it is ultimately not sustainable.[8]

The current approach to medical device inventories also falls short of organizational needs. Processes for collecting and compiling asset inventories of medical devices are largely manual and not standardized. Existing asset inventories also do not track the security posture (configuration, patching, and vulnerability scanning) of devices.

[8] Refer to the *Enterprise Cyber Security Strategy Team Domain Report: Medical Cyber – Cybersecurity Strategy and Implementation Plan for the Department of Veterans Affairs*.

2.2 MEDICAL DEVICES CYBERSECURITY PROJECT

The Cooperative Research and Development Agreement/Underwriters Laboratories (CRADA UL) Medical Devices Cybersecurity Project focuses on security for medical devices. It is part of a larger effort to foster knowledge exchange and partnership between VA, healthcare organizations, and medical device manufacturers.

One of the key goals of CRADA UL is to set criteria for VA medical device technology selection through a pre-certification program. Pre-certification reviews address both the hardware and software in medical devices. CRADA UL is also developing consistent OI&T-led processes for reviews and malware checks of medical devices.

2.3 VA INFORMATION AND ANALYTIC ECOSYSTEM

The VA Information and Analytic Ecosystem, managed by the Business Intelligence Service Line (BISL), is VA's designated enterprise service for analytics. Refer to the VA Enterprise Data Analytics EDP for an in-depth description of the Ecosystem, its current capabilities, and its planned future state. Section 3.4.2 describes the role that BISL and the VA Analytic Ecosystem will play in the proposed IoT program and VA's future IoT solutions.

2.4 VA ASSET MANAGEMENT SYSTEMS

VHA's Procurement and Logistics Office (P&LO) Service Oriented Architecture Research and Development (SOARD) project is replacing VHA's previous asset management system. Transition to the SOARD platform is currently[9] underway and will be complete by the end of 2018. The underlying commercial off-the-shelf (COTS) software of the SOARD platform is designed to track IoT assets as well as traditional IT assets. It also supports integration with other systems and platforms, including IoT platforms. It should be noted that the SOARD platform is not used to track clinical or patient-owned medical devices.

In addition, VA has a Real-Time Location System (RTLS) that supports automated location tracking for assets on VA premises via active Radio Frequency Identification (RFID) chips that broadcast their location. Most VA assets are tracked by scanning barcodes or passive RFID chips, and some are tracked via manual data entry. VA does not yet have a standard approach

[9] As of mid-to-late 2016.

to evaluating which types of assets require active tracking through RTLS versus passive or scan-based tracking.[10]

3 FUTURE CAPABILITIES

Table 2 maps the proposed capabilities described in this EDP to the problem or problems from Section 1.1 that they address.

Table 2: Mapping of Future Capabilities to Business Problems

Capability	Problem(s) Addressed	Purpose
Criteria for IoT Technology Selection and Approval	• *Poor endpoint device security* • *Emerging and rapidly evolving technology*	• Avoid or mitigate risks created by common IoT device security vulnerabilities • Ensure that devices are adequately maintained and supported by the vendor • Guarantee capability to update/patch device software and firmware
Device Isolation Architectures (DIA)	• *Poor endpoint device security* • *Distributed responsibility model*	• Limit potential damage of compromised IoT devices • Prevent use of compromised devices to attack VA networks
Comprehensive Asset Management for IoT Endpoint Devices	• *Poor endpoint device security* • *Difficulty of asset management* • *Distributed responsibility model*	• Inventory devices within and beyond VA organizational boundary • Provide visibility into device performance, configuration, and operational status • Maintain awareness of device ownership and management responsibility • Meet demand for devices while controlling costs

[10] A universal device location tracking approach may be addressed in a future design pattern.

Capability	Problem(s) Addressed	Purpose
IoT Solution Roles and Responsibilities	• *Difficulty of asset management* • *Distributed responsibility model*	• Define actors in IoT ecosystem to support IoT asset management • Shape Service Level Agreements (SLAs) with IoT vendors and service providers • Balances need for centralized management with local maintenance • Establish expectations for device end users
Enterprise IoT Help Desk	• *Difficulty of asset management* • *Distributed responsibility model* • *Emerging and rapidly evolving technology*	• Help projects and programs select appropriate IoT technologies • Enable multiple projects and programs to use the same IoT solution • Provide assistance and support to device end users • Serve as customer-facing component of VA enterprise IoT service

These capabilities will be provided and maintained by a designated VA enterprise IoT service provider (VAIoT) organization. This service provider may be part of, or a combination of, existing organizations such as the Enterprise Program Management Office (EMPO), BISL, MDPP, and HTM. The VA Chief Information Officer (CIO) will designate this VAIoT organization and provide it with the necessary resources and authority to implement the capabilities described in this EDP.

Refer to Section 3.4.1 for a list of VAIoT's responsibilities.

3.1 CRITERIA FOR IOT TECHNOLOGY SELECTION AND APPROVAL

Many networked embedded systems, including IoT endpoints, are not adequately engineered for cyber security. Many wirelessly networked "things" – from medical devices and industrial control systems to Wi-Fi-enabled baby monitors – have glaring security vulnerabilities such as:

- Use of nonrandom or default usernames and passwords
- Unnecessarily open network ports that create substantial attack surfaces
- "Bootstrap" Wi-Fi hotspots that do not require authentication and are never disabled
- Poorly encrypted or unencrypted connections to routers or other IoT devices
- Persistent open Telnet servers

- Lack of anti-malware protection

Some endpoints are simply unable to support security controls common in other technologies (such as laptops and smartphones) due to resource constraints. Other devices may not have such constraints, but for one reason or another security was simply not a consideration during the design process. Malicious actors can use poorly secured IoT endpoints to compromise the network the devices are on, even if that network is otherwise properly secured. Most of these insecure devices cannot feasibly be brought into compliance with VA security requirements through any sort of reconfiguration or compensating controls.

One approach to addressing this problem – the approach driving the CRADA UL Medical Devices Cybersecurity Project – is to simply avoid acquiring and using inadequately secured devices. The purpose of CRADA UL is to develop security-related certification and approval requirements for medical devices, similar to the requirements in the One-VA Technical Reference Model (TRM) software review and approval. CRADA UL will be responsible for pre-certifications and reviews of medical IoT devices.

VHA's Web and Mobile Solutions (WMS) will review non-medical endpoint devices that are associated with patient care. For example, fitness trackers issued to patients as part of care management or rehabilitation will fall under their purview. They will perform these reviews in coordination with VAIoT, and provide VAIoT with the results of their reviews.

VAIoT will be responsible for coordinating reviews of all other VA IoT devices. They will ensure that non-medical IoT endpoint devices (whether they are care-related or not) have TRM entries. IoT platforms operated by third parties on VA's behalf will be subject to the same review processes and requirements as other VA cloud services.

For the near future, VA will have to carefully vet candidate technologies, and may depend heavily on a relatively small number of devices that meet security requirements. As the IoT market and IoT-specific security best practices mature, VA will have a growing pool of potential technologies to choose from.

3.1.1 Requirements for all IoT Endpoints

All IoT endpoints will be fully documented in enterprise IoT asset management system. The system will retain records of all out-of-service IoT endpoints, as they do for medical devices. All configuration management, performance tracking, ownership, and location data/metadata associated with an endpoint device will be part of or associated with its asset management record.

To be approved for use by VA, future IoT endpoint devices will have either built-in or configurable capabilities to:

- Support tracking and continuous monitoring as described in this design pattern.
- Receive automated, authorized, digitally signed, over-the-air updates to its software, firmware, and configuration from the device vendor.
- Deny any network connections not explicitly permitted by the program or project deploying the device.
- Provide tamper detection for both hardware and software.
- Employ Federal Information Protection Standard (FIPS)-compliant encryption for data at rest and data in transit between the endpoint and its Field Gateway.[11]
- Have a unique device identifier, which will be used for asset management and identification/authentication purposes.
- Provide remote “killswitch” (i.e., memory wiping and/or disabling) functionality.
- Enable authentication via unique (not shared/default keys) in order to support:
    - Asset management
    - Access control
    - Device spoofing prevention
- Synchronize with a designated network time source in order to facilitate:
    - Time-stamping data points/alerts
    - Logging and auditing

An IoT endpoint will meet all of the above criteria regardless of where it is deployed or how it is used. Endpoint protection tools (e.g., for antivirus, antimalware, or file integrity checking) will be installed on any endpoints with sufficient compute capacity to support them. Additional criteria for a given IoT endpoint will depend upon whether the device is to be deployed on-site (within VA’s organizational boundary) or off-site (beyond VA’s organizational boundary).

Existing sensored facility management systems may not be able to meet all of these requirements. These devices will still be approved for use at VA, provided that they are connected using a Device Isolation Architecture (DIA) isolated from the main VA network (refer

[11] Some IoT devices may not be able to support existing forms of FIPS-compliant encryption due to processor or bandwidth constraints. NIST is currently exploring lightweight cryptography specifically for IoT devices. Future revisions of this design pattern will address acceptable types of lightweight cryptography, once they are available.

to Section 3.2). Any facility management systems or devices installed in the future will be subject to the technical requirements listed above.

For the foreseeable future, VA will refrain from enabling or using any “fog computing” or endpoint-to-endpoint analytics capabilities, due to security concerns. VA-owned endpoint devices will only communicate with designated gateways, and not directly with each other. This restriction may be lifted in subsequent versions of this EDP as IoT security matures.

3.1.2 Requirements for On-Site IoT Endpoints

An IoT endpoint will be categorized as “on-site” if it is deployed only within VA’s organizational boundary, i.e., at VA sites where it will connect to VA DIAs.[12] The DIAs will provide compensating controls to mitigate certain security vulnerabilities in on-site endpoints.

On-site IoT endpoint devices will:

- Support connection to a designated, appropriately configured VA DIA in such a way that it will be isolated from other IoT devices, VA networks, and VA IT assets.
- Be subject to location tracking, either through RTLS or scans when the endpoint is moved between areas of a facility or different facilities.

Any endpoint that is categorized as on-site will only be permitted to connect to specified and appropriately configured VA DIAs.

3.1.3 Requirements for Off-Site IoT Endpoints

An IoT endpoint will be categorized as “off-site” if it is deployed beyond VA organizational boundaries. An example is a fitness tracker issued to Veterans or VA employees: the device is intended for use outside of VA, and will have to connect to a network gateway that VA does not control. By definition, an off-site endpoint cannot rely on a DIA as a compensating control.

Therefore, devices will meet one or more of the following additional criteria in order to be categorized as off-site IoT endpoint devices:

- Supports end-to-end encryption between itself and a VA-designated IoT platform, regardless of the network gateway used.
- Connects only through one or both of the following methods:

[12] DIAs are described in greater detail in Section 3.2. In this document, the term “DIA” also refers to MDIAs, unless otherwise specified.

- Authenticated connection to a specified/known wireless network that will support an encrypted wireless connection.
- Authenticated Bluetooth connection to a specific device.

An IoT endpoint that is used both within and outside VA's organizational boundaries is considered an off-site endpoint. The same IoT endpoint may be an on-site endpoint in one use case and an on-site endpoint in another, depending upon how it is configured.

3.2 DEVICE ISOLATION ARCHITECTURES (DIA)

NIST recommends isolating ICS components (which have security issues similar to those of IoT devices) on dedicated network segments separate from the main corporate IT network.[13] "DIA" is VA's term for this type of network isolation approach, which mitigates some of the security vulnerabilities specific to IoT devices. Isolating endpoint devices reduces their risk of being compromised or used as a point of unauthorized entry into VA networks and other VA IT assets.

MDPP has a notional concept of DIAs for non-medical devices, but at this time the only VA DIAs in operation are MDIAs, which are exclusively for medical devices. As noted in Section 2.2, the current ACL-based implementation of MDIAs does not adequately meet existing needs for medical devices. It cannot scale up to support and secure non-medical IoT endpoint devices.

To better meet scalability and security needs for both medical and non-medical IoT endpoint devices, VA will transition to a new approach for implementing DIAs. DIAs will employ a "network separator" to isolate clusters of IoT endpoints from the main network and from each other. Network separators will reside on their own dedicated hardware, rather than relying on appliances used for VA's non-IoT assets. This does not preclude the use of appliances that are capable of supporting multiple isolated or logically separate networks for different clusters of IoT devices.

All network separators will incorporate a stateful inspection firewall. For particularly sensitive, high-impact, or intensively used IoT solutions VA will use a network separator consisting of both a stateful firewall and a router. Figure 3 illustrates the proposed DIA approach, with a network separator consisting of both a router and a stateful inspection firewall.

[13] Refer to NIST Special Publication (SP) 800-82 r2: *Guide to Industrial Control Systems (ICS) Security* (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf).

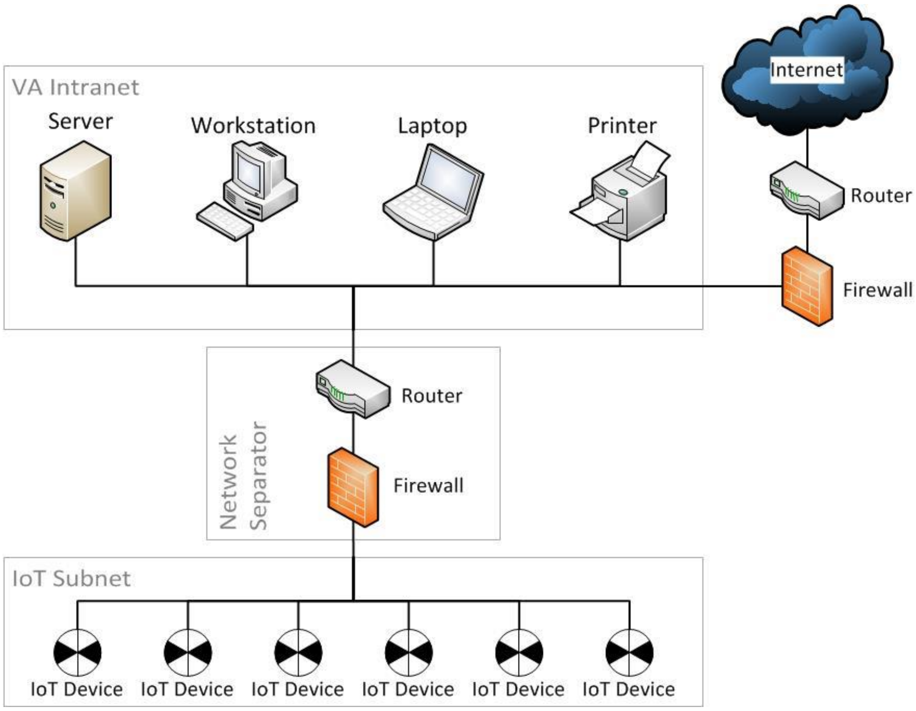

Figure 3: Device Isolation Architecture Diagram

Connections between endpoints in the DIA, and between the DIA and the main VA intranet, will operate in “deny-by-default” mode. Any ports or protocols not required to support the function of the endpoints or their associated IoT solution will be disabled. Similarly, IoT endpoints will only be permitted to connect with specific, whitelisted entities.

VAIoT will deploy and configure DIAs at VA sites in cooperation with local facility/site personnel. Rather than depending upon site personnel to manually set up DIAs, VAIoT will use mechanisms that support centralized/automated deployment and configuration. This will ensure scalable, repeatable, and compliant DIA implementation with minimal overhead. Authorized VA site personnel (such as facility CIOs, biomedical engineers, and equivalents) will be able to make configuration adjustments as necessary. Both centralized and local DIA deployments will be subject to an enterprise DIA change control process developed and maintained by VAIoT.

Separate DIAs will be deployed for medical and non-medical IoT devices. HTM currently determines the grouping of medical devices on separate MDIAs by function and/or manufacturer, and will continue to do so. VAIoT will follow a similar approach for non-medical IoT endpoints.

Individual clusters of endpoint devices will be connected to dedicated DIAs depending upon their function and any security capabilities and vulnerabilities identified during their review. In practice this will often translate to deploying different DIAs for different products from different manufacturers. This will help ensure that devices are connected to a DIA that provides both appropriate support for their functions and adequate controls for their vulnerabilities.

Most of the governance and process controls currently used for MDIAs will be used for non-medical DIAs as well. In particular:

- OI&T Enterprise Risk Management Office (ERM) assessment teams will perform ongoing validation of the implementation and management of DIAs as part of the sustainment of the Continuous Readiness Information Security Program (CRISP).
- The Isolation Architecture Change Approval Board (CAB) will support efforts to implement consistent change management practices, provide enterprise-level visibility, and improve the security posture of DIAs deployed across VA.

It should be noted that the DIA approach described in this section assumes that the devices on the DIA will connect via an Internet Protocol (IP) network, like traditional IT devices. However, dedicated IoT networks (such as 5G) currently under development by technology firms and cell carriers will prompt a reassessment of this approach in the near future. Subsequent revisions of this design pattern will address the use of standard or commonly used dedicated networks for IoT and how they should be isolated, if at all.

3.3 COMPREHENSIVE ASSET MANAGEMENT

Asset management will be a critical component of VA's IoT program. It is difficult to effectively manage and secure IoT assets (or any assets) if VA does not have enterprise-level visibility into its inventory. Comprehensive asset management of IoT devices will also support the accountability necessary to comply with security policies and other requirements.

VA will implement an enterprise-wide asset management system to track all non-medical IoT devices.[14] This system may either be part of VA's chosen IoT platform or under the direct management of VA itself. In the latter case, this EDP recommends modeling the asset

[14] Clinical and patient-owned devices will be tracked in separate systems under VHA's purview, following existing practice.

management system after the one currently being deployed by SOARD.[15] The VA CIO will designate an organizational steward for managing this system.

Asset management personnel within all VA LOBs will be able to use this system to manage IoT assets in their facilities or associated with solutions they own. This means they will be able to create and initiate asset management workflows appropriate to their business processes and IoT use cases.

All participants in the IoT asset management system will ensure that:

- All devices are completely and accurately documented, in compliance with this design pattern and any other requirements set by the asset management system's stewards.[16]
- Device records or parts of records are accessible to VA's IoTPSPs, sufficient to help them ensure the authenticity of IoT devices under their management.
- Any databases with supplementary data on IoT assets integrate with IoT asset management system, in such a way that all data about an endpoint device is linked to its asset management record.

VA will retain archival asset records for devices that have been taken out of service for a period of time (to be determined by OIS). These records will capture the “last known state” of the device, including the facility they were associated with (if not their exact location). These archived records will mitigate the risk of cyberattacks using spoofed or stolen endpoints and support forensics and discovery for investigating security incidents. Endpoint device records in or associated with asset management system entries will include information on the following:

- Operational status/state using available options in the asset management system.
- Configuration, including patch level and software version.
- Performance and diagnostics which may be used to automatically trigger asset management system work orders.

Asset management records for each endpoint device will also include, or be associated with, device location information. The best approach for tracking device location depends upon the

[15] And optionally using the same underlying software, as VA has an enterprise-wide license for as many instances as it chooses to deploy.

[16] As well as the Information Technology Service Management (ITSM) design patterns.

device capabilities, use case, and threat model.[17] The following approaches are recommended for tracking different types of endpoint devices:

- On-premise devices
    - Devices that remain in a fixed location in a VA facility will be tracked using one or both of the following mechanisms:
        - Connection to a specific facility network/DIA
        - Passive RFID chips or barcodes that are scanned periodically
    - Devices that are frequently moved around or between VA facilities will be tracked through RTLS using one or both of the following methods:
        - Location updates whenever the device connects to a VA facility network
        - Active chips that periodically broadcast the device's location (for expensive or high-value endpoint devices)
- Off-premise devices
    - Devices owned and operated by VA staff will be tracked through RTLS or Global Positioning System (GPS) *OR* associated with their designated end user
    - Devices issued to Veterans and beneficiaries will be associated with those individuals and their home address[18]

3.4 IOT SOLUTION ROLES AND RESPONSIBILITIES

This section provides a notional list of the roles involved in VA IoT solutions and what their responsibilities are. In some cases, the same individual or organization may play multiple roles with respect to a given IoT solution. Certain roles may also vary depending upon whether the IoT endpoint devices in the solution are on-site or off-site. Any role overlap or variance will be noted in the role descriptions below.

For certain solutions or use cases, particular responsibilities may be shifted to different roles than the ones described below, at the discretion of the VAIoT organization. Any IoT-related

[17] Consistent practice for location tracking may be addressed in a future design pattern.

[18] Specific identifying information for external end users (i.e., Veterans, their dependents, and beneficiaries) will be restricted by default to protect their privacy. VAIoT will work with VA Privacy Officers to develop appropriate access and disclosure requirements.

capabilities or requirements that are not specifically attributed to another party or organization are the responsibility of VAIoT.[19]

3.4.1 VA Enterprise IoT Service Provider (VAIoT) Organization

The notional VAIoT organization will be part of BISL. Its governance board will include representatives from BISL, the LOBs, and IoT Platform Service Providers (IoTPSPs) who manage IoT platforms for VA. It will be primarily managed by BISL.

The VAIoT organization has the following responsibilities:

- Manage IoT endpoint procurement and ensure that procured VAIoT endpoint devices are:
    - Documented in the IoT asset management system, from point of purchase through the end of their lifecycle.
    - Tracked through RTLS, network connections, or with bar codes, if on-site.
    - Tracked to/associated with designated end users, if off-site.[20]
- Develop, maintain, and enforce approval standards/requirements for non-medical IoT endpoint technologies, including:
    - Participating in technology review and approval processes.
    - Defining approval constraints and/or compensating controls for IoT endpoints.
- Provide specific contract language for use by technology vendors and IoTPSPs to guarantee their product and/or service’s adherence to security requirements.
- Develop, maintain, and enforce configuration requirements/standards for DIAs, in coordination with OIS and (for medical devices) MDPP and HTM.
- Assist VA facility and site personnel in deploying and configuring DIAs according to established requirements.
- Manage customer-facing IoT help desk for both end users and IoT data consumers (refer to Section 3.5).
- Provide implementation support to VA projects and programs seeking to set up new IoT solutions, or use existing ones that will supply the data they need.

[19] With the exception of technology selection/pre-certification requirements for medical IoT devices, which is the responsibility of the CRADA UL project.

[20] Specific identifying information for external end users (i.e., Veterans, their dependents, and beneficiaries) will be restricted by default to protect their privacy. VAIoT will work with VA Privacy Officers to develop appropriate access and disclosure requirements.

- Maintain a catalog of existing IoT solutions and data flows that may be shared with or used by multiple VA data consumers, in coordination with BISL.
- Facilitate reuse of existing IoT solutions to meet IoT data consumers' needs, where possible.
- Remotely disable and/or wipe endpoint devices that are reported as lost, stolen, or possibly compromised.
- Periodically conduct research on emerging IoT technologies, and submit promising ones to the appropriate review and approval process for consideration.

Any capabilities or requirements that are described in this EDP but not listed above are also the VAIoT organization's responsibility.

3.4.2 Business Intelligence Service Line (BISL)

BISL is VA's designated enterprise service provider for analytics. Their general duties and responsibilities with regards to analytics are described in the Enterprise Data Analytics EDP. They will carry out these same duties and responsibilities for data flows and analytic processes associated with IoT solutions.

In addition to managing VAIoT, BISL will have the following IoT-specific responsibilities:

- Establish, maintain, manage, and enforce contracts with IoTPSPs.[21]
- Manage and maintain any IoT platforms that are directly under VA's control, if applicable.
- Maintain a catalog of existing IoT solutions and data flows that may be shared with or used by multiple VA data consumers, in coordination with VAIoT.
- Cooperate with the IoTPSP to ensure immutability and integrity of data generated from IoT devices.[22]

3.4.3 IoT Platform Service Providers (IoTPSP)

As the name implies, IoTPSPs are responsible for the IoT platform component of an IoT solution. A platform service provider may operate a generic IoT platform, or they may operate

[21] The rationale for having BISL manage contracts with IoT platform service providers is that IoT platforms are (among other things) third-party analytics services. One of BISL's general responsibilities is to manage contracts with third-party (often cloud-based) analytics services.

[22] Data from IoT devices may still be deleted after aggregation or analysis is complete, depending upon the applicable use case(s) and project requirements.

one specifically for IoT endpoint devices they sell. In the latter case, the IoTPSP is also the IoT endpoint device vendor. This EDP recommends that VA rely as much as possible on generic IoT platform service offerings that can integrate with a large variety of IoT endpoint devices and other services.

IoTPSPs are subject to the same requirements as other Federal and VA cloud service providers, including those related to Federal Risk and Authorization Management Program (FedRAMP) certification.

IoTPSPs are also required to:

- Allow VA to perform management and orchestration of VA-owned/deployed IoT endpoint devices through their platforms.[23]
- Support authorized, digitally signed updates and patches to IoT endpoint device software/firmware, if such updates and patches can be deployed through the IoT platform.
- Coordinate with VAIoT – primarily the VA IoT help desk – to offer support to end users of VA-owned/deployed IoT endpoint devices.
- Keep VA apprised of planned updates, patches, or downtime for the IoT platform.
- Comply with Federal government and VA-specific requirements regarding data confidentiality, integrity, and availability, including data quality standards.
- Maintain, as part of the platform, an internal connection gateway to enable, mediate, and secure IoT endpoint device connections to the platform.
- Support "shadowing" of a large variety of IoT endpoint devices to address connectivity issues and provide consistent device interfaces. Device shadows will include:
    - The last known as-is state of the endpoint device.
    - The most recent data transmitted by the endpoint device (with time stamp).
    - The desired future state of the endpoint device.
- Ensure integration and ongoing compatibility of their platform with:
    - The VA Information and Analytic Ecosystem, under the direction of BISL.
    - VAIoT asset, performance, and configuration management processes and tools, to include tracking in the IoT asset management system.

[23] This requirement applies whether the platform is a generic IoT platform or specific to a particular type or subset of IoT endpoint devices (e.g., those manufactured by a certain vendor).

- In cooperation with BISL, ensure immutability of data generated from IoT devices, so that the data cannot be corrupted or tampered with.
- Through integration and cooperation with VA P&LO, ensure the authenticity of VA's IoT endpoints under management (i.e., that devices are legitimate and not spoofed).

Requirements for IoTPSPs, and their obligation to meet those requirements, will be explicitly defined in IoT service contracts.

3.4.4 IoT Endpoint Device Vendor (Vendor)

Endpoint device vendors are the firms that manufacture and sell IoT endpoint devices. In some cases they may also own and administrate the IoT platform for those devices, meaning they are IoTPSPs as well as vendors.

Vendors have the following responsibilities with regards to VA IoT solutions involving their products:

- Provide sustainment/support for products that VA has purchased and used throughout the products' lifecycle, to include:
    - Developing and automatically deploying digitally signed updates and patches to their endpoint device software/firmware to address known bugs and security vulnerabilities.
    - Assisting VA with maintenance of their products, including replacing defective or irreparably damaged products.
- Keep VA apprised of the following for any of their products VA has purchased and deployed:
    - Product recalls.
    - Newly discovered bugs or security vulnerabilities.
    - Planned updates and patches for device software/firmware.
- Furnish requested information to VAIoT (specifically the IoT help desk) so they can assist IoT data consumers and end users.

IoT vendors are also subject to all standard IT vendor requirements associated with VA asset management and the IoT asset management system.

Requirements for IoT technology vendors, and their obligation to meet those requirements, will be explicitly defined in IoT purchase and sustainment contracts.

3.4.5 IoT Data Consumer (Consumer)

IoT data consumers are projects and programs that consume data and business intelligence from IoT solutions. A consumer may be responsible for deploying a new IoT solution or they may simply be one of multiple data consumers for an existing solution. In the case of on-premise endpoint devices, the IoT data consumer role may overlap with the VA facilities and facility staff role (see Section 3.4.6).

IoT data consumers will coordinate with VAIoT whenever they initiate efforts to:

- Acquire and deploy a new IoT solution.
- Consume data from an existing IoT solution.
- Make changes to an existing IoT solution.
- Retire or transition away from an IoT solution.

If possible, consumers will use existing solutions that meet their data needs rather than deploying new but redundant solutions.

IoT data consumers are responsible for establishing incident response, contingency, continuity, and disaster recovery plans for the IoT solutions they deploy. Contingency plans for VA IoT systems – especially those used for safety-critical functions – will take into account the following principles:[24]

- Minimize the knock-on effects of component malfunction or failure.
  - Failed components should not generate unnecessary traffic in the IoT solutions or other networks.
  - A problem in one component should not cause another problem elsewhere, e.g., a cascading event.
- Engineer IoT systems for graceful degradation.
  - Normal, fully-automated operation.
  - Partial or emergency operation, with less automation and more involvement from human operators.
  - Fully manual operation.

[24] Refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 r2, *Guide to Industrial Control Systems (ICS) Security*, Section 2.3.1.

IoT data consumers that issue off-premise devices to external end users (such as Veterans) will also ensure that such end users are:

- Given instructions on care and maintenance for their devices.
- Provided with contact information for the IoT help desk.
- Informed about their responsibilities with regards to IoT endpoint devices in their possession (refer to Section 3.4.7).

3.4.6 VA Facilities and Facility Staff

VA facilities and facility staff are VA sites and site personnel where IoT endpoints are deployed, or they may be the closest available site to end users who have off-premise IoT devices. In some cases, these sites may be, or be part of, an IoT data consumer organization. The IoT-related duties of VA facility and facility staff include:

- Reporting any issues with IoT solutions (any component thereof) to VAIoT for recordkeeping and remediation.
- For all VAIoT devices:
    - Promptly submit appropriate work orders in the asset management system for broken, malfunctioning, disabled, or retired devices.
    - Facilitate or perform local on-site deployment and maintenance for devices as much as possible.
    - Make every reasonable effort to prevent damage to IoT endpoint devices on their premises.
    - Report any "orphaned" or unaccounted-for devices to VAIoT or the VA Procurement and Logistics Office
    - Ensure that endpoint devices are sanitized prior to being reissued or disposed of, similar to removable media.
- For on-premise IoT devices:
    - Ensure physical security for IoT endpoint devices to prevent them from being stolen or tampered with.
    - Facilitate and maintain proper configuration of devices and DIAs, to the extent possible.
    - Assist VAIoT in proper accounting for and maintenance of IoT devices.
- For off-premise IoT devices:
    - Ensure that off-premise devices do not connect to DIAs.
    - Provide direct assistance to external IoT end users if possible: otherwise direct them to the IoT help desk for assistance.

  - Pass on any end user reports of lost, stolen, damaged, or malfunctioning devices to the IoT help desk (through some automated means if available).

3.4.7 IoT Device End User (End User)

An IoT end user is the individual to whom an endpoint device is assigned or deployed. End users may be internal (e.g., clinicians, facility engineers) or external (e.g., patients). Not all IoT solutions will have an end user, as some IoT endpoints will be deployed in facilities rather than to individuals.

End users of IoT endpoints have the following responsibilities:

- Conduct device care/maintenance as recommended by the IoT consumer and/or facility that deployed the IoT endpoint device.
- Take all reasonable precautions to prevent the IoT device from being lost, damaged, or stolen.
- Do not give or lend the IoT endpoint device to unauthorized users, i.e., someone who is not the designated end user/recipient of the device.
- Promptly report a lost, stolen, damaged, or malfunctioning IoT endpoint device to either the IoT help desk or the nearest VA facility.

3.5 ENTERPRISE IOT HELP DESK

The IoT help desk, run by VAIoT, will serve as a “second tier" to the National Service Desk (NSD) that deals specifically with IoT-related assistance. The help desk will provide support and instructions to the following roles and organizations (in order of priority) with IoT-related issues:

- End users
- Facilities and facility staff
- IoT data consumers
- BISL
- IoT vendors and IoTPSPs

To fulfill its duties and provide adequate support to its customers, the IoT help desk will employ the following enterprise resources:

- VA’s Customer Relationship Management (CRM) Unified Desktop
- The IoT asset management system, to initiate asset management work orders for IoT devices

- Diagnostic and management functions (as appropriate) in VA's IoT platforms

3.6 ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM)

All projects will leverage the approved tools and technologies located in the VA TRM[25] to comply with the architectural guidance provided in this document. **Error! Reference source not found.** lists the approved tools for this EDP.

Table 3: List of Approved Tools and Standards for Internet of Things Technologies

Technology Category	Example Technologies	Example Standards	Mandated ESS
IoT Endpoint Devices	*N/A*	*N/A*	*N/A*
IoT Platforms	*N/A*	*N/A*	*N/A*
Asset Management	IBM Maximo Asset Management	*N/A*	*N/A*

The TRM is a component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the IT used to develop, operate, and maintain enterprise applications. The TRM serves as a technology roadmap and tool for supporting OI&T. TRM reviews may be performed on IoT platforms and the software in IoT endpoints, but not the hardware. Refer to the Data Storage EDP for a description of the TRM review and approval process.

3.7 ALIGNMENT TO VETERAN-CENTRIC INTEGRATION PROCESS (VIP)

VIP is a Lean-Agile framework that serves the interest of Veterans through the efficient streamlining of IT delivery services that occur within the enterprise. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely and predictably. VIP is the follow-on framework from Project Management Accountability System (PMAS) for the development and management of IT projects which will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

More information can be found here (https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/).

[25] http://trm.oit.va.gov/

4 USE CASES

4.1 OFF-PREMISE IOT DEVICE ISSUED TO A VETERAN

4.1.1 Purpose

This use case illustrates a basic architecture and set of information flows for an off-premise IoT device issued to a Veteran – specifically, a fitness tracker. It is also an example of a solution in which some of the data analytics are performed close to the IoT endpoint and its user. The fitness tracker may have been issued to the Veteran as part of a rehabilitation or wellness program.

In this particular case, both the non-VA end user and VA clinical staff can see the results of analytics from the data source (i.e., the IoT endpoint device). However, they may not see the same data or see it in the same time frame. The end user will receive near-real-time analysis and updates, while VA staff may only see a historical record that is updated on a daily basis.

4.1.2 Assumptions

- The fitness tracker has been issued to the Veteran by VA.
- The Veteran can see their current and historical fitness data on their smartphone, which is connected to the fitness tracker.
- FIPS-compliant encryption is used to secure data at rest and in transit from end-to-end throughout the entire IoT solution.
- Data transmitted by the fitness tracker consists of telemetry and some device metadata. None of the user's personally identifiable information is transmitted.
- The IoTPSP that manages the IoT platform in the solution does not share the Veteran's data with any party other than VA and the Veteran.[26]

4.1.3 Use Case Description

- The fitness tracker collects data and makes it directly available to a mobile application on the Veteran's smartphone via Bluetooth.
- Mobile application performs some simple analytics on fitness tracker data (e.g., number of steps taken, current heart rate).
- Mobile application sends data to the IoT platform.

[26] The Veteran may "opt in" to sharing the data with other services or devices, but by default data sharing from the device is restricted.

- The IoT platform performs analysis on the data supplied by the fitness tracker through the Veteran’s smartphone and transmits the results of analysis:
  - Back to the Veteran’s smartphone, either automatically (push model) or when the Veteran requests it (pull model).
  - To VA for further analysis and recordkeeping, possibly along with original telemetry data from the fitness tracker.
- VA analyzes and/or stores Veteran’s fitness data transferred by the IoT platform. The data goes to two different consumers within VHA:
  - Clinical staff. For them, the Veteran’s fitness data is associated with their electronic health record (EHR).
  - Researchers. They receive the same data as the clinical staff, but it is de-identified – they cannot tie it back to a specific person.

4.1.4 Use Case Context Diagram

Figure 4 below illustrates the flow of data between components in the use case. Note that the flow of data into the EHR and medical research databases is unidirectional. The flow of data (and analytic output) between other components is bidirectional.

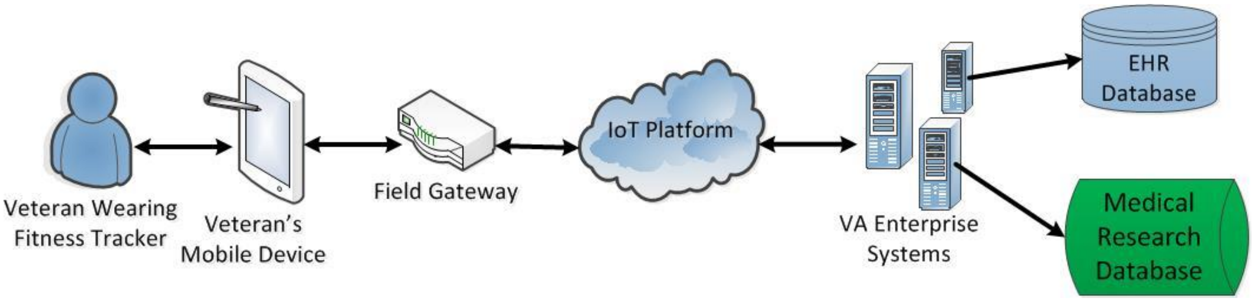

Figure 4: Illustration of Off-Premise IoT Device Issued to a Veteran

4.2 ON-PREMISE IOT DEVICE FOR FACILITY MANAGEMENT

4.2.1 Purpose

This use case focuses on a sensor unit in the cooler of a VA facility’s Heating, Ventilation, and Air Conditioning (HVAC) system. The sensor supports two different data collection functions:

- Sensing, and sending alerts about, the presence of harmful biologics (e.g., Legionella) in the Heating, Ventilation, & Air Conditioning (HVAC) system.
- Providing telemetry on the function of the cooler for facility management and preventive maintenance purposes.

Because of the dual function of the sensor unit, the IoT solution includes analytic workloads at both the Endpoints (i.e., in the sensor) and Enterprise Back-End components.

4.2.2 Assumptions

- The cooler and sensor unit are functioning properly.
- The sensor is on a dedicated facility DIA for components of the HVAC system.
- Telemetry is sent to both plant managers for the facility and the VA central office.

4.2.3 Use Case Description

- Sensor takes periodic readings from the HVAC cooler.
- Sensor unit performs simple analytics on readings to determine whether biologics are present in the cooler. If so, the sensor unit sends an alert to the local plant manager.
- During normal operations the sensor unit sends telemetry that goes back to the asset management platform for preventive maintenance purposes.

APPENDIX A. SCOPE

This EDP describes proposed capabilities for managing and securing IoT solutions within the VA enterprise. Topics include:

- Technology selection and approval criteria for non-medical IoT devices:
    - For on-premise devices connected to VA networks
    - For off-premise devices deployed to external end users
- Baseline requirements for DIAs
- IoT endpoint asset management:
    - Tracking devices in VA's new asset management system
    - Configuration, ownership, operational, performance, and location tracking
- Roles and responsibilities for IoT solutions:
    - VA enterprise IoT manager
    - Projects, programs, and LOBs that deploy and use IoT devices
    - Vendors and third-party IoTPSPs
    - Local VA facilities and technicians
    - External end users
- Enterprise IoT help desk to facilitate IoT support and information sharing

The following concepts are outside the scope of this design document:

- Technology selection and certification requirements for medical devices
- Analytic processes beyond IoT platforms[27]
- Specifics of applications and services that will support:
    - IoT orchestration and maintenance
    - Device hardware, firmware, and software
    - Deploying, configuring, and managing DIAs
- Infrastructure and hardware design specifications
- Vendor-specific technologies

[27] This topic is addressed in the *Interoperability and Data Sharing: Enterprise Data Analytics* EDP.

A.1 DOCUMENT DEVELOPMENT AND MAINTENANCE

This EDP was developed collaboratively with internal stakeholders from across the Department and included participation from VA 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, Veterans Benefits Administration (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

Actuator – Actuators such as control valves, breakers, switches, and motors are used to directly manipulate controlled processes based on commands from back-end business systems, which are based on analysis of data input from IoT sensors.

Authenticity – A property guaranteeing that a device and/or the data associated with that device is legitimate and accurately reflects the subject's origins and purpose.

Data Flow – Describes the lifecycle and movement of data in an analytic system (as part of or including an IoT solution) with respect to a particular process or use case. A data flow begins with collection/ingestion from data sources and ends with the presentation of information extracted from the data using reports, visualization tools, applications, etc.

Endpoint *or* Endpoint Device – The endpoint is the actual "thing" in the Internet of Things. Endpoint devices almost always include some type of sensor, and they may include one or more actuators as well.

Enterprise Backend – In the context of an IoT solution, the enterprise backend consists of enterprise applications and services (including the complex analytics capabilities) that process data sourced from the endpoints.

Gateway – A device or service through which an IoT service connects to a/the network. Depending on the use case, the gateway for a device may be a desktop or laptop computer, a smartphone or tablet, a router, or a specialized IoT device hub.

Immutability – A property of data generated by or associated with an IoT endpoint device (or any other data source). If such data is immutable, that means it has not been corrupted or subjected to unauthorized changes.

Ingest, Ingesting, *or* Ingestion – The entry of raw data input into the analytic system from data sources, to include applications, operational data stores, feeds, sensors, etc.

Platform – In the context of an IoT solution, a platform is a service that provides data ingestion and device management for IoT endpoints. It may also perform some of the analytics on data ingested from IoT endpoint devices.

Sensor – Device that produces a measurement of some physical property and then sends this information as controlled variables to the platform and back-end business systems.

Shadow – A placeholder for an IoT endpoint device in an IoT platform and/or asset management system. The shadow records the last known current state and the desired future state of the device. Shadows provide a stable connection point for a device that is encountering connectivity issues. A shadow also allows applications that depend on the device to operate normally even if the device itself is not available.

APPENDIX C. ACRONYMS

Acronym	Description
ACL	Access Control List
ADS	Authoritative Data Source
ASD	Architecture, Strategy and Design
CAB	Isolation Architecture Change Approval Board
COTS	Commercial Off-The-Shelf
CRADA UL	Cooperative Research and Development Agreement/Underwriters Laboratories
CRISP	Continuous Readiness Information Security Program
CRM	Customer Relationship Management
DBMS	Database Management System
DIA	Device Isolation Architecture
EA	Enterprise Architecture
EDP	Enterprise Design Pattern
EHR	Electronic Health Record
EPMO	Enterprise Program Management Office
ERM	Enterprise Risk Management Office
ESS	Enterprise Shared Service
FDA	Food and Drug Administration
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Protection Standard
FISMA	Federal Information Security Management Act
FSS	Field Security Services
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HISD	Health Information Security Division
HTM	Healthcare Technology Management
HVAC	Heating, Ventilation, and Air Conditioning
IoT	Internet of Things
IoTPSP	IoT Platform Service Provider
IPv6	Internet Protocol Version 6
ITSM	Information Technology Service Management
LOB	Line of Business
MDIA	Medical Device Isolation Architecture
MDPP	Medical Device Protection Program
NIST	National Institute of Standards and Technology

Acronym	Description
NIST SP	National Institute of Standards and Technology Special Publication
OI&T	Office of Information and Technology
OIS	Office of Information Security
P&LO	Procurement and Logistics Office
QoS	Quality of Service
RTLS	Real-Time Location System
SD&E	Service Delivery and Engineering
SOA	Service-Oriented Architecture
SOARD	Service Oriented Architecture Research and Development Project
TLS	Transport Layer Security
TRM	Technical Reference Model
VA	Department of Veterans Affairs
VAIoT	VA IoT Service Provider Organization
VA-MDNS	VA Medical Device Nomenclature System
VHA	Veterans Health Administration
VIP	Veteran-Centric Integration Process
VLAN	Virtual Local Area Network
WMS	Web and Mobile Solutions

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 EA:

#	Issuing Agency	Applicable Reference/ Standard	Purpose
1	VA	VA Directive 6551	Establishes a mandatory policy for establishing and utilizing Enterprise Design Patterns by all Department of Veterans Affairs (VA) projects developing information technology (IT) systems in accordance with the VA's Office of Information and Technology (OI&T) integrated development and release management process, the Veteran-focused Integration Process (VIP).
2	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in VA, which applies to all applications that leverage ESS.
3	VA Deputy Assistant Secretary for Information Security	Certification of Medical Devices in Medical Device Isolation Architecture (MDIA) Memorandum	Establishes Department-wide requirements for deploying, configuring, and maintaining MDIAs.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
4	VA Deputy Assistant Secretary for Information Security	Updated Security Requirements for Network Connected Medical Devices and Systems (VAIQ #7566605)	Establishes updated requirements, including procurement processes and training programs, related to medical devices and MDIAs.
5	VA OIS FSS	Medical Device Isolation Architecture (MDIA) Implementation Analysis	Describes deficiencies in the current approach to MDIA implementation and recommends a proposed solution to address these deficiencies.
6	VA ECST	ECST Domain Report: Medical Cyber Cybersecurity Strategy and Implementation Plan For the Department of Veterans Affairs	Report on the current state of VA medical device security and recommendations for addressing identified deficiencies in the medical cyber domain.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
7	NIST	NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	Applicable to protecting the confidentiality of controlled unclassified information (CUI): • When the CUI is resident in nonfederal information systems and organizations • When the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and • Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry.
8	NIST	NIST SP 800-82 r2: Guide to Industrial Control Systems (ICS) Security	Outlines concepts, considerations, and best practices for networked embedded systems that are also applicable to IoT systems.