

VA IDENTITY PRODUCT

Sprint 3 Demo

Wednesday, September 28, 2022



U.S. Department
of Veterans Affairs



The Discovery team

Core team, design research



Kit Casey
Design Director



Samara Watkiss
Assoc. Design
Director



Pablo Cruz
Sr. Product
Manager



Mike Prusaitis
Assoc. Director,
Program Management



Steve Dickson
Engineering Lead,
Key Personnel



Bri Mazzio
Sr Interaction
Designer



Marissa Klein
Sr. Strategist



Paul Knipper
Visual Designer



Elizabeth Koch
Product Owner,
Key Personnel

Executive team



Jeff Scheire
MO Studio



Travis Hoffman
MO Studio



Kevin London
Frog Design

Key Personnel joining the team



Name: Tyler Gindraux (Blue Tiger)

Role: Sr. User Experience Researcher

Start Date: 10/17/2022

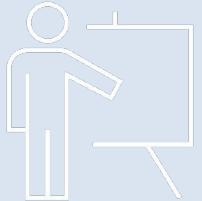
Location: South Carolina

<https://www.linkedin.com/in/tylergindraux/>

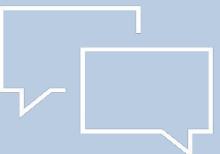
At the end of each sprint on Wednesday, the team will run sprint reviews to showcase the sprint's work for approval.

The purpose of this meeting is:

1 To demo the accomplishments or functionality that was accomplished over the past sprint



2 To get feedback and insights early and often



3 To create transparency for anyone interested on the product and progress



Goals and agenda

Sprint 3 goal

- e-QIP background checks
- VFS Platform orientation
- Collect follow up materials from interviews
- Upcoming interviews: Inherited Proofing, TAP (Melissa R. and Dr. Hill)
- Identify any additional business owners or SMEs related to focus areas, schedule interviews, prep conversation guides as needed
- Connect team with MHV coordinators, kiosk PO (⚠)
- Identify opportunity areas for field research
- Collaboration Cycle:
 - *Submit Collaboration Cycle Request*
 - *Prep Design Intent/Research Review*
- Github + Zenhub set up

Today's agenda

- | | |
|---------------|---|
| 10 min | Discovery Phase status |
| 30 min | What we've learned so far (interviews) |
| 10 min | Security & compliance matrix |
| 8 min | Status: Non-Veteran user roles, flow documentation, and security keys |
| 2 min | Next steps |

Areas of focus

Priority 1

MHV Coordinators in person proofing (and remote video)

MHV Coordinators have direct contact in-clinic with Veterans nationwide, and therefore have greater understanding of various challenges Veterans face. MHV Coordinators have potential to guide the migration toward login.gov especially for Veterans needing in-person proofing.

Priority 2

Non-Veteran user roles focusing on Caregivers, Beneficiaries, and Delegates

There are hosts of non-Veteran users that would require login.gov and related identity proofing. Currently there are no VA-wide agreed upon definition of these users or clarity on their use cases and needed levels of access. The primary user roles to investigate are delegates, caregivers, and beneficiaries. These individuals will need the ability to identity proof in person at VA facilities.

Priority 3

Inherited proofing/Migration of MHV users to login.gov

There is an opportunity to leverage previous identity proofing to streamline the transition to login.gov for existing users. Differing security standards of legacy proofing options will what is required to meet Login.gov standards. The end goal is to simplify the migration process for existing users.

Priority 4

Security keys in-person proofing (in place of MFA)

Some users struggle with using Multi Factor Authentication. Could MHC Coordinator to provide these users with security keys as an alternative?

Priority 5

TAP curriculum evaluation

The TAP curriculum is out of date when it comes to login for VA services and benefits. It should be updated to remove DS logon and encourage users to use login.gov from the start. *This area has unknowns, a lack of contact points and relationships, and a lack of general knowledge.*

Business owners and SMEs consulted

Completed interviews

- Carnetta Scruggs: MHV
 - Management Analyst and Technical Liaison
- Sonja Skinner: MHV
 - MHV Coordinator & VA Medical Center Visit
- VSP Team: Account Migration
 - Nick Soutouras, Ian Hundere, Joe Niquette, Alex Johnson, Amanda Porter, Afia Caruso, Trevor Bosaw
- Dr. Carla Hill: TAP
 - Program Analyst, Curriculum
- Melissa Rebstock: VBA, VBO
 - Director - My HealtheVet at Department of Veterans Affairs
- Dr. Berkowitz: Data and Ethics
 - Sr Ethicist - VHA National Center for Ethics in Health Care
- Matt Baum: Health Data Security
 - Senior Health Data Security Specialist at Veterans Health Administration
- Coordinators Focus Group #1: MHV

Upcoming interviews

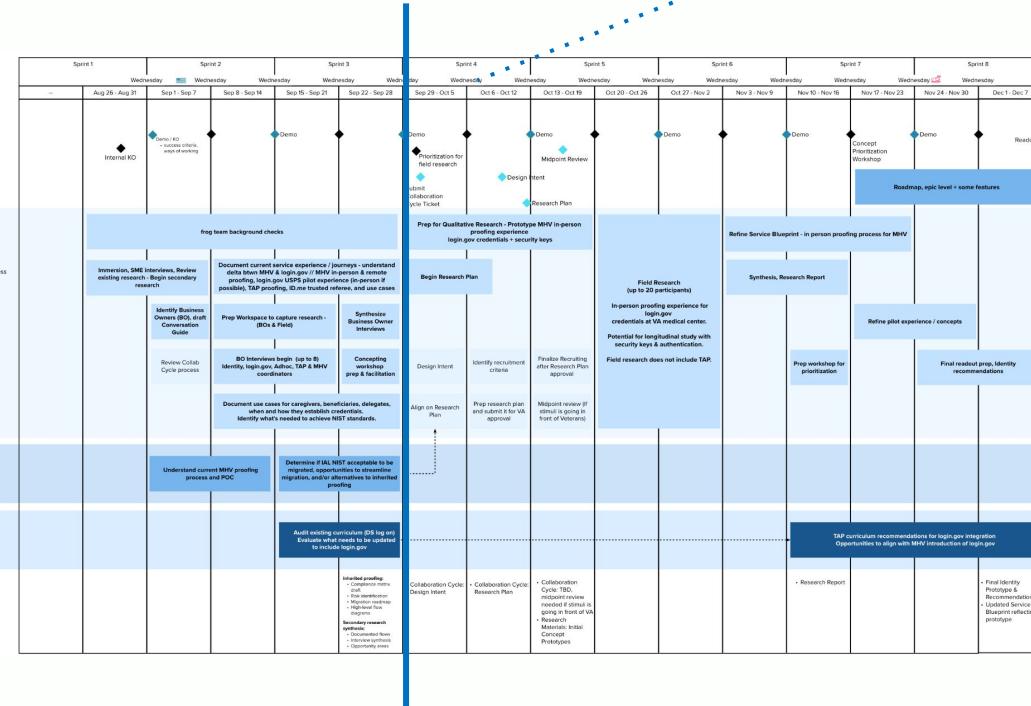
1. Laurie Baker: VBA, VACO
 - Senior Management Analyst
2. Coordinators Focus Group #2: MHV
3. VHIC subject matter expert

On hold

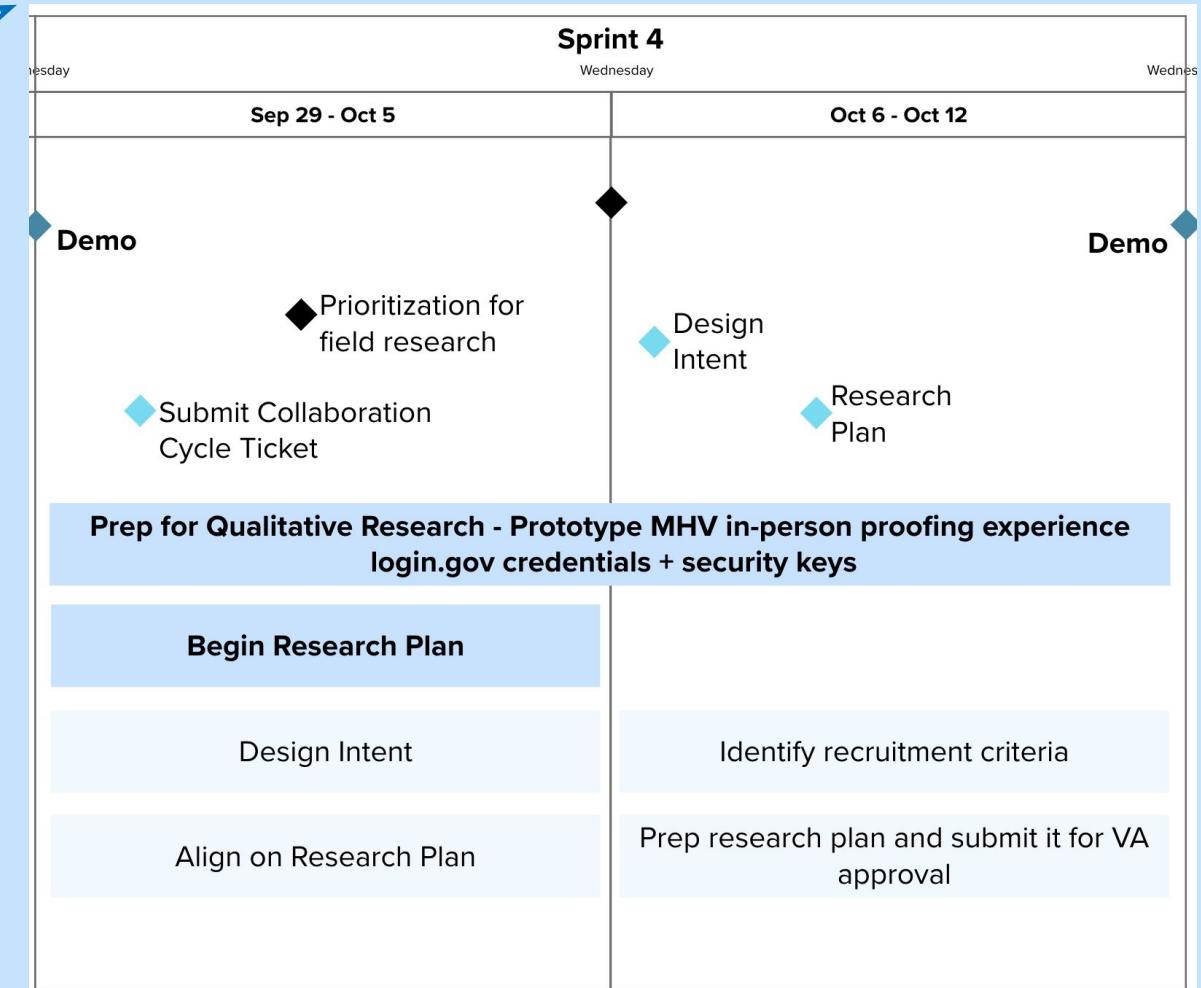
N/A

Our plan

We are here



A closer look to the sprint ahead...



Dependencies, risks, blockers

Dependencies:

- Getting team fully through VA onboarding (orientation)
- Field Research Prep & Collab Cycle
 - starts Oct 26
- Velocity Tracking
 - VA Github + Zenhub instance creation
- Travel Planning (if required for research)

Risks:

- N/A

Blockers:

- VA larger file & videos access (requires google access)
 - o MP to investigate

What we've learned so far

1. Carnetta Scruggs - *MHV*
2. Sonja Skinner - *MHV Coordinator & VA Medical Center Visit*
3. VSP Team - *Account Migration*
4. Dr. Carla Hill - *TAP*
5. Melissa Rebstock - *VBO*
6. Dr. Berkowitz - *Data and Ethics*
7. Matt Baum - *Privacy and Security*



Carnetta Scruggs - MHV

Interview Objective

Understand the processes, roles, user experience, and challenges around setting up and accessing a My HealtheVet premium account. In particular focusing on:

- MHV coordinators & in-person proofing
- USPS Pilot
- Multi-factor authentication options and challenges
- Veterans' experiences with MHV account creation and access
- Non-Veterans' experiences with MHV account creation and access

Interviewee

Carnetta Scruggs

Management Analyst and Technical Liaison for the Office of Connected Care Veterans and Consumer Health Informatics Office

“Should I help this Veteran and their wife get their account, or do I say no?... It’s a moral dilemma they are in.”

Carnetta Scruggs

“You gotta get delegates... they're having their wife, their kids, their neighbor log in for them. We want to know who's logging in for them, so they need a delegation path.”

Carnetta Scruggs

Carnetta Scruggs - Key Takeaways

1. MHV Coordinators feel the need to bend the rules and find creative workarounds in order to provide quality and efficient care for Veterans.
2. The current system is designed in a way that sets up elderly, disabled, rural, and homeless Veterans for failure. Not providing the necessary human and technological assistance further marginalizes these groups.
3. Service providers and doctors are impacted by a lack of delegate solutions. Doctors are unsure who they are communicating with and what they can legally share.
4. Not all VAs are created and maintained equally, adding to Veteran's confusion when interacting with the VA.
5. Partnering with USPS hopes to remove barriers and increase access for harder to reach Veterans—a benefit to both Veterans and the VA.
6. Friends and family are instrumental in assisting Veterans who are aging, have mental and physical health issues, and technical literacy challenges. A lack of delegate consideration means this assistance comes at the expense of security and proper protocol.



Sonja Skinner - MHV Coordinator

Interview Objective

Understand how, in her particular context of the Tyler VA Medical Centers, she conducts in-person proofing and helps Veterans access their MHV accounts. In particular focusing on:

- Support for basic account creation
- Process for in-person proofing
- Remote trusted referee proofing
- Multi-factor authentication options and challenges
- Veterans' experiences with MHV account creation and access
- Non-Veterans' experiences with MHV account creation and access
- Understanding of related roles, facility, artifacts, tools

Interviewee

Sonja Skinner

My HealtheVet Coordinator - VISN 17/Central Texas, VAOS Schedule Manager

“[Ideally] they click the upgrade button and it just works. They already have the VHIC. It would be ideal if they didn't have to come in.”

Sonja Skinner

“There really is no benefit to having a basic account. Unless you just want to journal.”

Sonja Skinner

Sonja Skinner - Key Takeaways

1. Basic MHV accounts serve limited/no purpose and make account creation a convoluted two-step process resulting in user frustration.
2. Enlisting and training primary care staff and administrators opens up the opportunity for identity verification any time a Veteran is checking in for an appointment or interacting with a provider.
3. Because of the rigorous process required to get a VHIC, sometimes coordinators will check for a VHIC on file when by-the-book methods of proofing are difficult. There is the opportunity to include proofing for MHV access with applying for a VHIC.
4. An estimated 60% of those who seek help with in-person proofing have tried to proof online first. The current systems is proving unusable for a wide variety of people, not just the elderly or those unfamiliar with technology.
5. Although all staff can act as verifiers and there are a number of other authenticators, many staff are in the habit of sending all in-person proofing to the MHV coordinator, who is also the primary source for help troubleshooting problems with access, and so becomes a bottleneck.
6. Detailed asynchronous resources (PDF and youtube tutorials) are an opportunity to alleviate the need for 1:1 and/or in-person assistance.



VSP Team - Account Migration

Interview Objective

Understand the current state of the inherited proofing work to migrate accounts from MyHealtheVet credentials to Login.gov credentials. In particular focusing on:

- VSP team make up and their experience collaborating with other teams
- Eligibility requirements for account including in the migration pilot
- Status of development with inherited proofing
- Challenges faced with inherited proofing

Interviewees

Nick Soutouras

Senior Product Manager at Oddball

Ian Hundere

DevOps Engineer at Oddball

Joe Niquette

IT Security at Oddball

Alex Johnson

Front End Engineer at Oddball

Amanda Porter

UX Researcher at Oddball

Afia Caruso

Front End Engineer at Oddball

Trevor Bosaw

Back End Engineer

“[The number of users eligible for auto migration] is a drop in the bucket.”

Joe Niquette

[On MFA options] “Text & voice, face & touch were most popular among participants.”

Amanda Porter

VSP Team - Key Takeaways

1. Only a small subset of premium users (~200k users) have been identified so far as eligible to participate in pilot. The VSP team does not determine the qualifications for eligibility for migration, nor do they know all of the requirements for eligibility.
2. What is known is that eligible users have gone through in-person proofing and have an “ID on file”. Login.gov is considering the risks associated with accepting these account as-is, or requiring additional proofing steps for IAL2 compliance.
3. Initial pilot will take lessons learned & can be applied to MHV premium users who have DS Logon and ID.me accounts before migrating to Login.gov.
4. User testing is being conducted on the auto-proofing flow that users whose accounts are being migrated would experience. In general feedback has been positive and possible sources of confusion have been identified.
5. VSP team is following NIST and ICAM requirements.



Dr. Carla Hill - TAP

Interview Objective

Understand TAP processes, roles, user experience, and challenges, with specificity around setting up and accessing of VA-based accounts. In particular focusing on:

- TAP Benefits Advisors training and responsibilities
- Existing TAP curriculum content and update process
- Current TAP schedule ie. agency order
- Non-Veteran users' participation in TAP
- Veteran experience with account creation during TAP

Interviewees

Dr. Carla Hill

Program Analyst, Curriculum
VA Transition Assistance Program
(TAP)

Cordelia Postell

Program Analyst, TAP Curriculum &
Policy

"[It's] just nearly impossible [to retain] a 200 page document that you're going through in one day."

Dr. Carla Hill

"I am not aware of any centralized place where [the various support role trainings] all come together."

Dr. Carla Hill

Dr. Carla Hill - Key Takeaways

1. The lack of coordination between DOD TAP training and VA TAP training creates redundancy and confusion, especially around login options.
2. There are multiple options for how to access TAP training (in-person, online, async) and variations of course content - without clear information about which approach is most effective TAP leaders prioritize.
3. VA TAP curriculum is due for a tech-capable, user-friendly upgrade.
4. TAP classes walk Veterans through the process of signing into certain accounts, but this training does not extend to accessing MHV Premium.
5. Although not official policy, trainers are encouraging Veteran spouses to participate in TAP training. Because family members and caregivers are key in accessing Veteran benefits, TAP can explore more formalized training for non-Veteran users.
6. Training for Veteran support personnel (TAP Benefits Advisors, VSOs and MHV Coordinators) is decentralized. An opportunity exists to ensure training resources are centralized and complimentary.



Melissa Rebstock - VBA, VBO

Interview Objective

Understand the processes, roles, user experience, and challenges around setting up and accessing Veteran benefits. In particular focusing on:

- Veteran setup of eBenefits and challenges with access
- Non-Veteran users' needs and roles
- Addition of alternate credential options: Login.gov and ID.me
- Multi-factor authentication options and challenges

Interviewees

Melissa Rebstock

Branch Chief for Digital Modernization Division in the Multi-Channel Technology Directory of the Veterans Experience Office

“We focus so much on Veterans, but we don't pay enough attention to their families.”

Melissa Rebstock

“Biggest complaint: Veterans can be transferred [while on the phone] but don't have a direct number to call, so what happens when the call drops?”

Melissa Rebstock

Melissa Rebstock - Key Takeaways

1. Alignment of training materials is critical for both Veterans and VA staff members especially when considering turnover.
2. Investing time in more engaging and accessible training materials will prevent unnecessary asks on staff time.
3. There is not a clear delineation between Veterans and associated non-Veteran users, especially those that might fulfill dual or multiple roles within a Veteran's life. By establishing these roles, it will help set context of how staff can more effectively assist them, reducing confusion and uncertainty for all parties.
4. A clear, accessible path to support is essential. Veterans' access to their benefits, particularly DS Logon, is challenging and unreliable, even if they already have an account. There is a lack of or non-existent technical support, preventing access at critical moments.
5. There are key moments for Veterans to start the credential process *prior* to when it's an essential need in their lives—before they exit the service. It should be a simple process to re-establish a credential at the time of need.



Dr. Berkowitz - Data and Ethics

Interview Objective

Understand the key data and ethics issues relating to accessing a My HealtheVet premium account, and the challenges of migrating to only allowing access through Login.gov and ID. me. In particular focusing on:

- MHV coordinators & in-person proofing
- Multi-factor authentication options and challenges
- Veterans' experiences with MHV account creation and access
- Sharing Veteran information with caregivers and delegates
- Balancing security and accessibility

Interviewee

Dr. Berkowitz

Sr Ethicist - VHA National Center for Ethics in Health Care

VA DGC Data Ethics Workgroup Associate

Co-Chair EHRM Ethics Council

“We need to balance security and over-security... If we create systems that create barriers and leave people out, we are failing our fundamental mission.”

Dr. Berkowitz

“We are sort of forcing people to do the wrong thing, so we should design a system to do the right thing.”

Dr. Berkowitz

Dr. Berkowitz - Key Takeaways

1. MHV Coordinators Education is necessary, but insufficient. A culture change is also necessary, so that Coordinators and Security teams keep the bigger picture in mind, and do the right thing by all Veterans.
2. Trust is key and requires transparency, true consent, ethical use of data, and user choice.
3. We need to solve for the last 5% of Veterans who are hardest to reach (rural, homebound, or unwilling to alter their digital practices), and will require special accommodations and additional resources to meet them where they are.
4. We must design the system to support well intentioned users, not the bad actors. A system that does not provide realistic options for all users sets well-meaning individuals up to break the rules.
5. There must be a balance between security and over security. If a login is so secure but creates insurmountable barriers to services, we have failed our primary mission of serving the Veteran.



Matt Baum - Health Data Security

Interview Objective

Understand the key security and compliance issues relating to accessing a My HealtheVet premium account, and the challenges of migrating to only allowing access through Login.gov and ID. me. In particular focusing on:

- Protection vs. over-protection, balancing security and accessibility
- Multi-factor authentication options and challenges
- Veterans' experiences with MHV account creation and access
- Sharing Veteran information with caregivers and delegates
- Connected care considerations

Interviewee

Matt Baum

Senior Health Data Security Specialist
at Veterans Health Administration

“[Getting login right] is the foundation of getting everything else right.”

Matt Baum

“Privacy requirements drive security requirements (not the other way around).”

Matt Baum

Matt Baum - Key Takeaways

1. Be realistic and mindful of the large/complex user base when deciding, building, and implementing solutions. Focus on the full experience of ALL users (from onboarding, authenticating, proofing, service, support, offboarding, etc.).
2. Just because the VA, as an organization, needs to follow Federal policy, remember that Veterans do not—they are considered part of the general population.
3. Data Ownership dictates which Privacy Policies apply to whom—which consequently influences Security requirements.
4. While Veterans experiencing homelessness (lowest common denominator) know how to take advantage of public facilities and associated benefits (e.g. Library internet access), MFA will still remain a challenge in regards to phone number and email. *Username and password*, will need to remain an option or we risk excluding a large number of Veterans.
5. There's an opportunity to explore using the VIC card as a secondary means of authentication as part of logging in.
6. The current credential process (for MHV) is onerous and repeats steps required for other applications in the VA ecosystem. There's potential to leverage security measures across applications in the VA ecosystem.



In Progress: MHV Coordinators Group Conversations

Interview Objective

Understand the variety of contexts where MHV coordinators work, the challenges they encounter, and workarounds they employ to get users access to MHV. In particular:

- Type of facility and demographic
- Main challenges with accessing MHV
- Approaches and tools created to support Veterans in accessing MHV
- Experience working with non-Veterans
- Experiences and concerns with login.gov and MFA
- Suggestions and hopes for future login options

Research Plan

Session 1 - completed

5 MyHealtheVet Coordinators
Monday September 25, 2022

Session 2 - scheduled

4-6 MyHealtheVet Coordinators
Friday September 25, 2022



Security & compliance matrix

Objective

Help inform decisions regarding additional proofing steps with the inherited proofing process and other solutions for migrating existing MHV Premium accounts with consideration of NIST SP 800-63A IAL2.

Process

- Primary focus is on in-person proofing (remote proofing requirements are grayed-out)
- Map 800-63A IAL2 Requirements for the MHV in-person proofing process
- VHA 1907 Compliance
- VHA 1907 Reference/Evidence
- MHV In-person proofing compliance
- MHV In-person proofing evidence, e.g. *Training materials and Stakeholder interviews*

Next steps

- Analysis and counts of MHV premium accounts and types of identity proofing used, including whether primary and secondary IDs used for In-Person proofing
- Assess if there's parity of ID.me and Login.gov (Terms and Conditions)

Considerations

- Degree of interpretation of Compliance
- Policies indicate what is supposed to be which may differ from reality of what is currently implemented
- Training documentation reflects what is currently implemented but isn't a complete picture

Security & compliance matrix: High-level diagram

(Detailed Excel to be delivered via email following this meeting)

Create
Basic MHV
account →

Upgrade Process to Premium MHV account		Verification process	Meets NIST 800-63a standards?
Upgrade Online	Use DS Logon Premium Account to ID proof	Proofing process for premium accounts uses knowledge-based questions	✗
Upgrade Online	Use ID.me account to ID proof (prior to IAL2)	ID proofing compliant with 800-63-2	✗
Upgrade Online	Use ID.me account to ID proof (post update to IAL2)	ID proofing compliant with 800-63-3	✓
Upgrade In-person or by phone <i>(Unknown, we are speculating if this option was ever allowed based on VHA policy.)</i>	Older MHV In-person proofing that uses Knowledge Questions	No ID presented	✗
USE CASE FOR MIGRATION LOGIN.GOV PILOT (VSP TEAM)			
Upgrade In-person <i>(~200,000 users)</i>	Newer MHV In-person proofing that requires primary and/or secondary IDs	ID verified in-person	✗

Security & compliance matrix: Key takeaways

- The MHV in-person proofing interface is IAL2 compliant in that it does *not* allow knowledge-based questions, however VHA policy still allows for this if both primary and secondary forms of evidence are not available
- Following MHV in-person proofing practices relating to identity evidence are not IAL2 compliant:
 - *VIC cards are FAIR evidence strength yet allowed as a single primary evidence for MHV in-person proofing, whereas a STRONG+ or SUPERIOR evidence are the only IAL2 compliant options for a single ID evidence*
 - *Drivers License is STRONG evidence strength and has been allowed as a single primary evidence for MHV in-person proofing (Note that REAL ID cards are STRONG+ and are IAL2 compliant as a single ID evidence)*
 - *In cases where there is a mismatch with the VA record and the primary ID evidence, a single form of FAIR evidence is allowed for MHV in-person proofing, whereas, for IAL2 compliance, two forms of FAIR evidence are required in addition to the STRONG primary*
 - *ID cards are not vetted with the issuing source*
- **To be IAL2 compliant, MHV must confirm address (phone, postal or email);** however, the MHV in-person proofing has no process to collect or confirm address as part of the in-person proofing process
- MHV in-person proofing process supports different types of ID evidence with varying strength.
There are opportunities to define inherited proofing eligibility based on type of primary evidence that was used during MHV in-person proofing



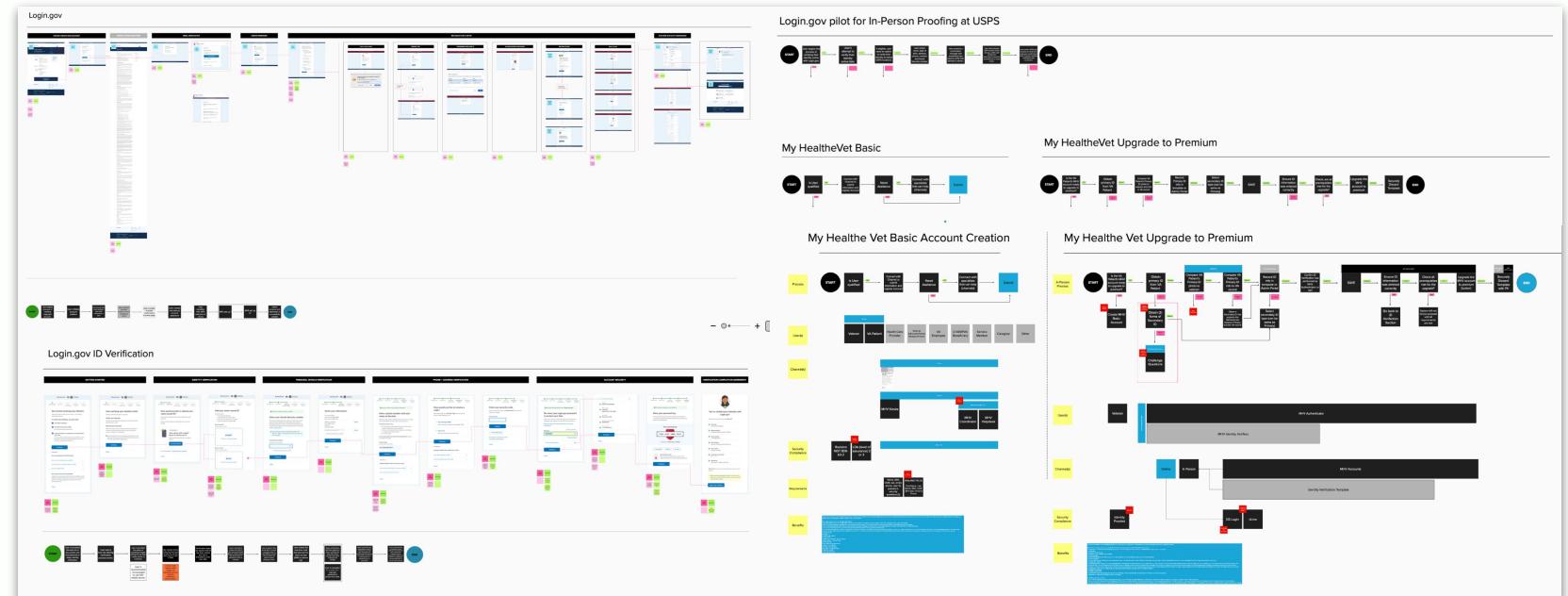
Flows documented

Objective

Gain a holistic understanding of the implemented proofing process (for MHV, login.gov, USPS pilot and MHV premium account migration with respect to security and compliance) and identify opportunity areas to streamline migration to login.gov and improved in-person proofing.

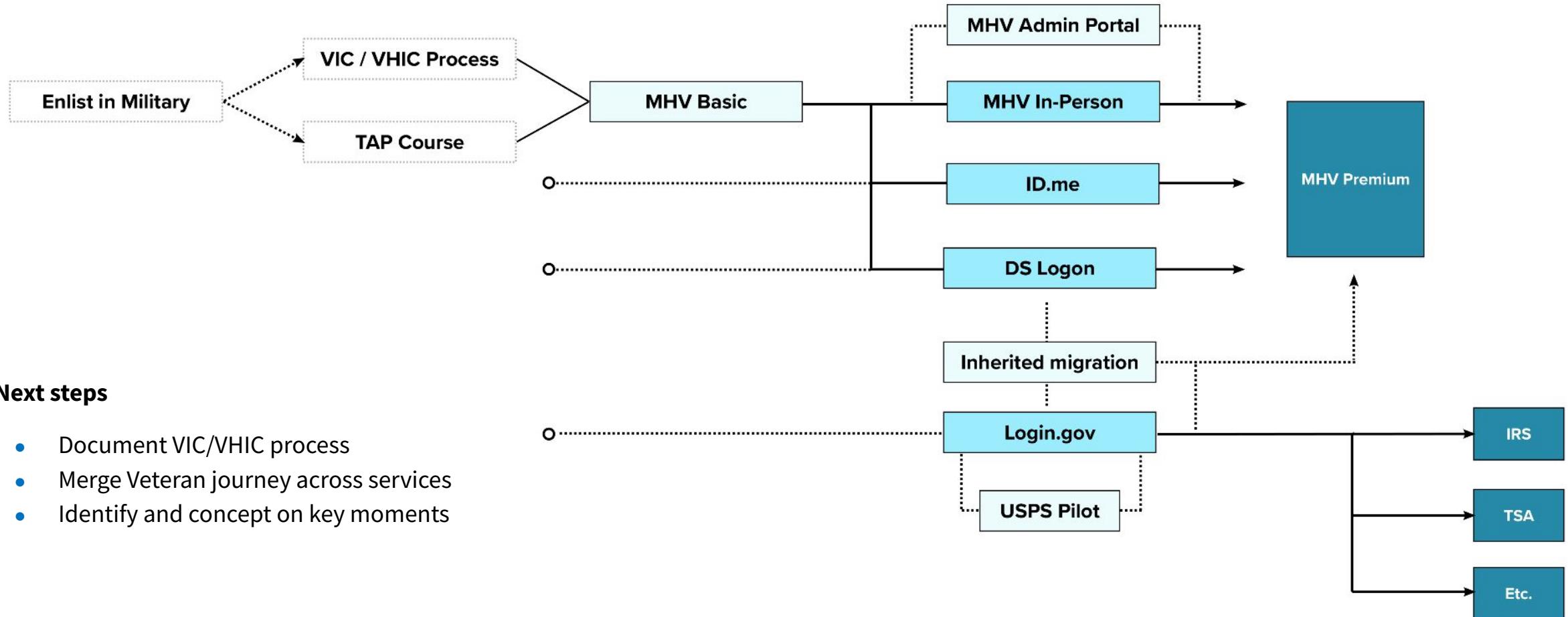
Flows documented so far

- MHV Basic
- MHV Premium
- Login.gov Online
- Login.gov USPS Pilot
- MHV Inherited Migration



Where we're heading...

Bird's Eye View



Next steps

- Document VIC/VHIC process
- Merge Veteran journey across services
- Identify and concept on key moments

Status: Non-Veteran User-roles

Objective

There are hosts of non-Veteran users that would require login.gov and related identity proofing. Currently there are no VA-wide agreed upon definition of these users or **clarity on their use cases and needed levels of access**.

The primary user roles to investigate are delegates, caregivers, and beneficiaries. These individuals will need the ability to identity proof in person at VA facilities.

Process

- Started documentation of what we know
- Completed & integrated notes primarily from the MHV and TAP-focused interviews
- Reviewed the Non-Veteran User Roles Discovery Readout and supporting research

In-progress

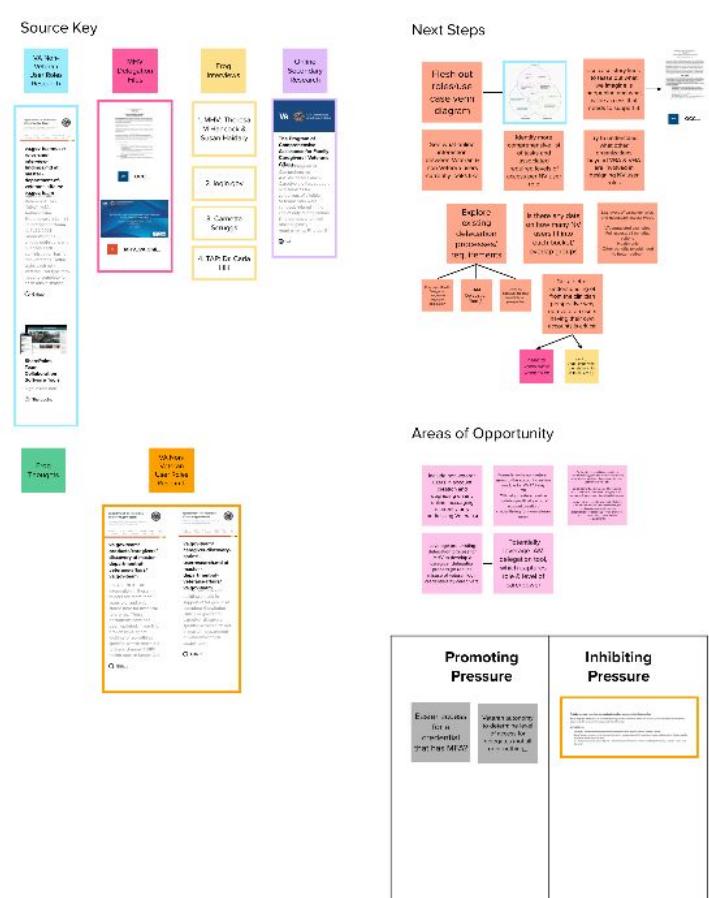
- Secondary research outside of VA-produced materials
- Review of the MHV delegation research materials provided by Carnetta and the MHV team
- Understanding the overlap of roles and needed levels of access
- Review of the Discovery for Program of Comprehensive Assistance for Caregivers from Shawna Hein & UX team
- Explore promoting and inhibiting pressures of Non-Veteran separate account creation

Open questions

- Are there any individuals who are the primary point person for Non-Veteran users?
- What is the ideal end state/goal?
 - What are the ideal levels of differentiation between roles and respective access?
- What compels a non-Veteran user to set up their own account?
 - How would having their own account make providing care easier/more accessible? (And how might it encourage a Veteran to direct their delegates/caregivers down this path vs. simply sharing a password?)

Status: Non-Veteran User-roles

Non-Veteran User Roles



Status: Security Keys

Summary of findings

In general, the stakeholders and business owners we have spoken to have not been very familiar with security key and no one we have spoken to has tried providing them to Veterans as an option for MFA.

- MHV coordinators have been steering Veterans away from login options that require MFA, not exploring alternative methods of MFA
- Veterans who already have security keys or are familiar with them are unlikely to need help with MFA
- Veterans who do need assistance with account set-up and MFA are not suggesting or asking about security keys

Next steps

- Complete and integrate desktop research findings
- Determine possible path for testing:
 - Security key training material for MHV coordinators
 - Messaging and training material to facilitate self set-up of security keys
 - Providing a security key and supporting set-up as part of TAP

Open questions

- How long would it take a MHV coordinator or similar role to help a Veteran set up a security key?
- Would it be possible to mail a Veteran a security key and either with printed material, videos, or a live video call help the Veteran set-up the security key?
- What is the price point for buying security keys in bulk?
- What are the recovery options for a lost security key?

Next steps

Sprint 4 goals

- VFS Platform orientation
- MHV Coordinator Focus Group #2
- Upcoming interviews: Laurie Baker
- Prep for Field Research
 - Research Plan Creation & Validation
 - Concept Ideation & Narrowing
- Collaboration Cycle:
 - Submit Collaboration Cycle Request
 - Prep Design Intent/Research Review

Questions?

VA IDENTITY PRODUCT

Appendix

Strengths of Identity Evidence References

NIST 800-63a Reference

IAL2-2 (4.4.1.2)

The CSP SHALL collect the following from the applicant:

1. One piece of SUPERIOR or STRONG evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR
2. Two pieces of STRONG evidence; OR
3. One piece of STRONG evidence plus two pieces of FAIR evidence

IAL2-6a (4.4.1.6 #2)

The CSP SHALL confirm address of record.

Strength	Method(s) Performed by the CSP
Unacceptable	<ul style="list-style-type: none">• Evidence validation was not performed, or validation of the evidence failed.
Weak	<ul style="list-style-type: none">• All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.
Fair	<ul style="list-style-type: none">• Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s), OR• The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, OR• The evidence has been confirmed as genuine by trained personnel, OR• The evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.
Strong	<ul style="list-style-type: none">• The evidence has been confirmed as genuine:<ul style="list-style-type: none">○ using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, OR○ by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified, OR○ by confirmation of the integrity of cryptographic security features.• All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	<ul style="list-style-type: none">• The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features.• All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

Materials received to-date

APRIL 2022

Identity MHV Inherited Eligible Users Study readout

This research will inform design, content, and functionality changes needed to address any pain points within the flow of the inherited proofing process and to potentially uncover accessibility needs on VA.gov. **Recommendations:** Additional support for iOS/macOS, education for VA advocates & social workers, video-tutorials/FAQs.

JAN 2022

Identity Sign-in Accessibility Study readout

To discover issues or pain points when using a screen reader (and other assistive technology) to login using the sign-in modal on VA.gov.

Recommendations: Reduce page content, improve navigation, find solution for Caregivers/Family to securely sign in w/o sharing PII, integrate assistive tech.

NOV 2021

User Roles research findings

Three primary non-Veteran user groups: Beneficiaries, Caregivers, Delegates. **Recommendation:** Conduct additional research to identify use cases, tasks, and outcomes for each of these non-Veteran user groups.

OCT 2021

Identity VA.gov Sign In Modal readout

To understand how the addition of Login.gov and other design modifications to the VA.gov sign-in modal will impact a user's ability to sign in; understand what information Veterans, find the most important or least important in a sign in option; understand which type of credential provider would users prefer, given the choice of government-created or private sector. **Recommendation:** Look to simplify CSP buttons, share ranking attributes to guide communications around changes to providers

SEPT 2021

Identity Authentication Discovery readout

To understand the potential impact of sunsetting providers such as MHV and DS Logon. **Recommendation:** Use sentiment around other providers and account creation process to build case Login.gov is most secure provider

DEC 2015

Credentials Final Readout Master No PII

To understand how users currently log in to VA.gov and why they use one credential over the other (MHV, DS Logon, and ID.Me)

Materials received to-date

AUG 2022

LE Project Discovery Report, Priority Life Experiences

Research conducted to better-understand the physical, mental, and emotional needs of Transitioning Service Members (TSMs), Recently Separated Veterans (RSVs), and their families during Military to Civilian (M2C) transition.

Associated deliverables:

2022

Transition Journey Map

This journey map depicts the Service member experience navigating military to civilian transition, and the impact of activities and events within that journey on their future.

2022

Transition Personas

To discover issues or pain points **when using a screen reader** (and other assistive technology) to login using the sign-in modal on VA.gov.

Recommendations: Reduce page content, improve navigation, find solution for Caregivers/Family to securely sign in w/o sharing PII, integrate assistive tech.

SEPT 2022

In-Person Proofing Pamphlet for TMF Partners.pdf

Login.gov overview of the upcoming pilot for in-person proofing, in partnership with USPS. The partnership leverages USPS's current informed delivery workflow and existing infrastructure.

Additional documentation found

2022

MHV Authenticator Role Training - via TMS

Roles and responsibilities of a MHV Authenticator, including the role of an Identity Verifier. Process to upgrade a MHV account to Premium (In Person and Online).

APRIL 2021

MHV Identity Verification - VHA Directive 1907.02

This Veterans Health Administration (VHA) directive establishes mandatory standards for verifying the identity of a Veteran or others (e.g., delegates, guardians, personal representatives) requesting a My HealtheVet (MHV) Premium account for the highest level of access to individually-identifiable health information (IIHI) within MHV. This verification process includes responsibilities for Department of Veterans Affairs (VA) medical facility MHV Coordinators or other staff assigned to perform identity verification.

May 2022

MHV Proofing Interface

This solution will enable Veterans who have already completed the MHV in person verification process to automatically transition their verification information over to a login.gov account.

2022

OIT Vision 2022

Assistant Secretary for Information and Technology and Chief Technology Officer Kurt DelBene defines his vision for the future of OIT.

2022

MHV Upgrade to Premium - via MyHealth.gov

Dedicated public website dedicated to educating users on the benefits of Premium and how to upgrade.

2022

VA Handbook 6510

This Handbook defines roles, responsibilities, and procedures to implement VA Directive 6510, VA Identity and Access Management, for the Department of Veterans Affairs (VA).

THE BIGGER PICTURE

Identity mission, objectives, and product vision

Mission and objectives

Mission

The CEDAR IDIQ will connect VA employees with industry partners to deliver high-quality, digital products following modern best practices to improve service delivery to Veterans.

Objectives

- Give VA streamlined access to a small group of exceptional companies that specialize in agile software development and user-centered design
- Create a contract mechanism that incentivizes VA employees and contractors to deliver rapidly following private sector best practices
- Promote the principles of Agile and DevOps culture in VA
- Support VA's digital modernization strategy to solve tough technology challenges facing VA

Product vision

VISION

- One sign-on to access all products and services.
- Veteran choice of “public” or “private” credential option for VA.gov

HOW

- Use human-centered design to consolidate ways to sign on to VA.gov
- Migrate users to their choice of Login.gov and ID.me; robust, compliant credential solutions

WHY

- Users are frustrated and confused because they must go to multiple websites for benefits
- Multiple ways to sign on adds to the confusion
- Current sign on options have usability, security, and compliance issues

TO ACHIEVE THIS, WE NEED TO DELIVER ON...

Simplicity

Veterans need a simple way to access all VA sites

Guidance

Veterans need efficient customer service

Trust

Veterans believe there is an inherent risk to submitting sensitive information via the internet

Continuous discovery and Veteran feedback

Taking time to continually test and validate through prototyping

Adherence to standards

Compliance with standards such as NIST 800-63-3

SPRINT 2

What we've learned so far

Evolution of Focus

FROM

1. Define Non-Veteran user roles (*e.g., dependents, beneficiary, caregiver, delegate, VSO representatives, claim agents and attorneys, fiduciary, Power of Attorney (POA), 3rd-party organizations that receive payments*)
2. MHV Coordinators in person proofing (and remote video)
3. Inherited Proofing/Migrate users in Premium status
4. Update Transition Assistance Program (TAP) Curriculum to remove DS Logon and include Login.gov
5. Email/comms outreach for DS Logon MFA rollout

TO

1. MHV in-person (and remote) proofing process
2. Non-Veteran user roles focusing on Caregivers, Beneficiaries, and Delegates
3. Inherited proofing/Migration of MHV users to login.gov
4. Security keys in-person proofing (in place of MFA)
5. TAP curriculum evaluation

My HealtheVet

Interview Objective

Understand the processes, roles, user experience, and challenges around setting up and accessing a My HealtheVet premium account. In particular focusing on:

- MHV coordinators & in-person proofing
- The relationship between basic and premium accounts
- Remote trusted referee proofing
- Multi-factor authentication options and challenges
- Veterans' experiences with MHV account creation and access
- Non-Veterans' experiences with MHV account creation and access

Interviewees

Theresa M Hancock

Director - My HealtheVet at
Department of Veterans Affairs

Susan Haidary

National Stakeholder Manager at
Department of Veterans Affairs

“[Getting login right] is the foundation of getting everything else right.”

Theresa M Hancock

“To get the full suite of what My HealtheVet has to offer, all the bells and whistles, every feature they need to have a premium account.”

Susan Haidary

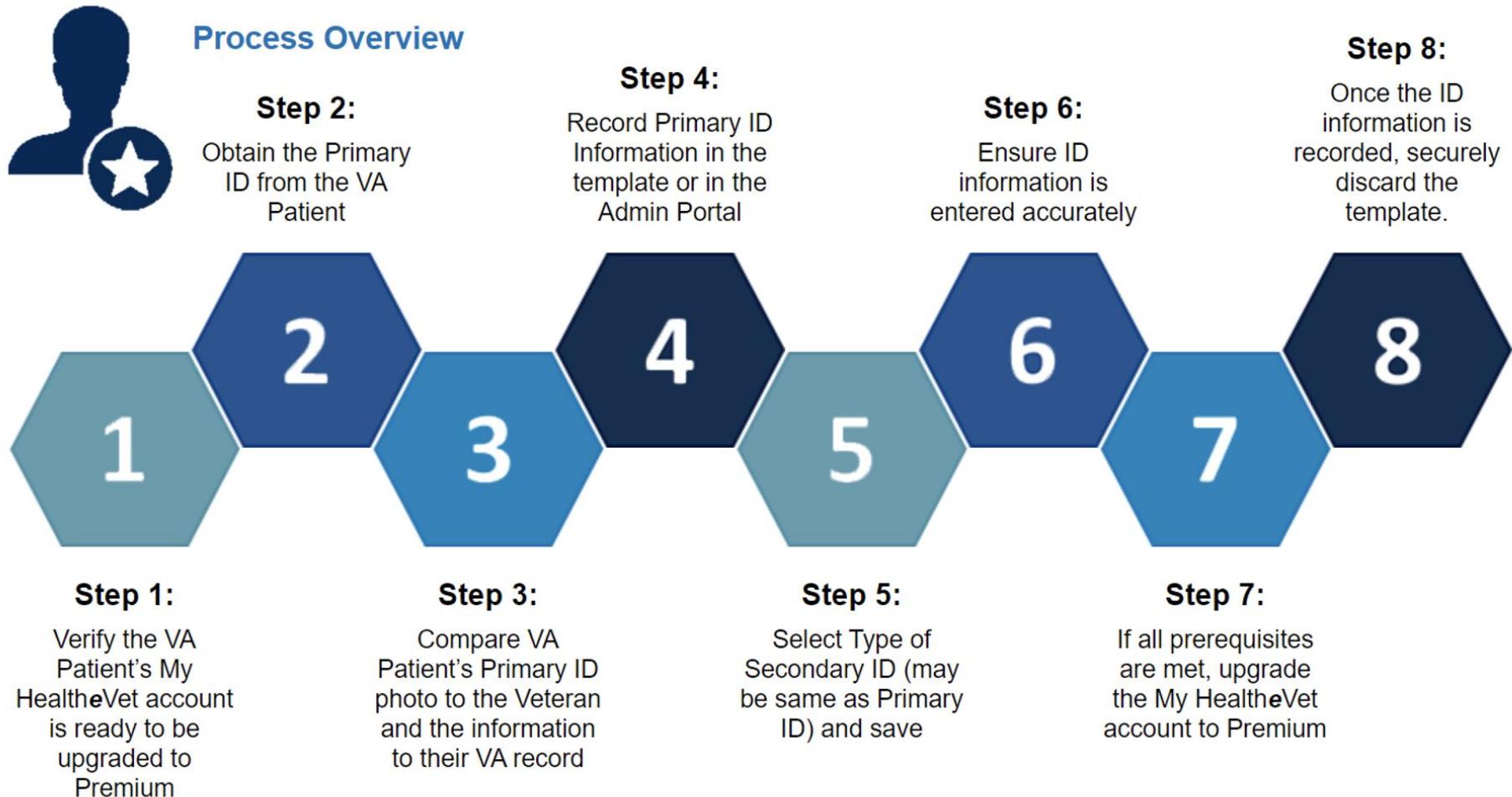
My HealtheVet - Key Takeaways

- Providing access options that work for all Veterans is top priority, without access Veterans cannot use the benefits or services available to them
- Basic account setup is the first step to a premium account and often requires in-person support
- Premium MHV accounts require identity proofing, and allow users to access medical records, communicate with providers, and order prescriptions
- The reality is that caregivers access MHV using Veteran credentials, so MHV needs to plan for it, not forbid it
- MHV staff only recommend what they feel comfortable using and teaching, so timely training is key
- Veterans feel unheard and rate usability as very low—a surprise to those who built login and MFA solutions

MHV premium users

	My HealtheVet Basic	My HealtheVet Premium
Requirement	<ul style="list-style-type: none">- Anyone can register on My HealtheVet starting with a Basic account.- A Basic account provides limited access to features in My HealtheVet that you self-enter	<ul style="list-style-type: none">- Once your account is connected to your VA/DOD records, your account can be upgraded to Premium
Process	<ul style="list-style-type: none">- Can be done online or in-person at VA Medical Center <p>Online via My HealtheVet:</p> <ul style="list-style-type: none">- Complete the registration form—information collected: Name, DOB, SSN, Gender, Email Username, Password- Accept the Terms and Conditions- Select Create Your Account button	<ul style="list-style-type: none">- Can be done online or in-person at VA Medical Center- Online: Must create ID.me (IAL2)/DS Logon to complete identity proofing- In-person: You'll need to bring a government-issued photo ID. This can be either your Veteran Health Identification Card or a valid driver's license.- If the primary ID information does not match the users official VA medical record, a secondary form of ID, such as a social security card, is required.- Resources: local My HealtheVet Coordinator, a member of Veteran's VA health care team, My HealtheVet Help Desk

MHV premium users: In-person upgrade



*MHV Authenticator Role Training - via TMS

MHV premium users

	My HealtheVet Basic	My HealtheVet Premium
Benefits	<p>Access to your personal information located in VA or DoD systems. With a Basic account you may use My HealtheVet to:</p> <ul style="list-style-type: none">- Add information to a personal health journal about over-the-counter medications, allergies, military health history, medical events, tests, and allergies- Record and track personal information such as contact information, emergency contacts, health care doctors and providers, and health insurance information- Record and track personal health measurements (blood pressure, blood sugar, cholesterol, heart rate, body temperature, weight, pain level, etc.) in Vitals and Readings- Print a health insurance wallet ID card with the personal information entered into the personal health record- Set personal goals. My Goals makes it easy for you to set goals, identify your strengths and tasks, to overcome obstacles, and track your progress. My Goals can be used to help your VA health care team understand what is important to you.- Use the VA Blue Button (Download My Data) to view, save, print, or download and save your self-entered information; then share this with your caregiver, non-VA provider or others you trust. Your self-entered information may include:<ul style="list-style-type: none">- Activity Journal- Allergies- Family Health History- Food Journal- Health Care Providers - Health Insurance- Immunizations - Labs and Tests- Medical Events- Medications and Supplements- Military Health History- My Goals: Current Goals- My Goals: Completed Goals- Treatment Facility- Vitals and Readings	<p>Upgrading to a Premium account gives users full access to My HealtheVet features. With a Premium Account you may use My HealtheVet to view key portions of your VA health record, such as:</p> <ul style="list-style-type: none">- VA Admissions and Discharges (including discharge summaries) - Discharge Summaries are available 36 hours after they are completed- VA Allergies- VA Appointments (future)- VA Appointments (limited to past 2 years)- VA Demographics- VA Electrocardiogram (EKG) (EKG dates are no longer updated. You may continue to view your historical EKG dates.)- VA Immunizations- VA Laboratory Results: Chemistry/Hematology/Microbiology - VA Laboratory Results are available 36 hours after they have been verified. Depending on the type of test, some laboratory results may not be available right away.- VA Medication History- VA Pathology Report: Surgical Pathology/Cytology/Electron Microscopy. VA Pathology Reports are available 36 hours after they have been completed. Some studies done at a non-VA facility may not be available or they may not necessarily include an interpretation.- VA Problem List - Your VA Problem List contains active health problems your VA providers are helping you to manage. This information is available 36 hours after it has been entered. It may not contain active problems managed by non-VA health care providers.- VA Notes - VA Notes written from January 1, 2013 forward are available 36 hours after completion and signed by all required members of your VA health care team. Compensation and Pension exam notes will be available 30 calendar days after they are completed.- VA Radiology - Your report is available 36 hours after it has been verified by members of the VA health care team- VA Vitals and Readings- VA Wellness Reminders- VA electronic health record information such as VA Continuity of Care Document (VA CCD) and other information as it becomes available- Department of Defense (DoD) Military Service Information <p>In addition you may be able to:</p> <ul style="list-style-type: none">- Use the VA Blue Button to view, save download and/or print your VA health and DoD Military Service Information. You can also share this with your caregiver, non-VA provider or others you trust.- Download your VA Continuity of Care Document (VA CCD). This is a standard electronic exchange document, used for sharing patient information. The VA CCD will be a summary of important health information from the Veterans VA Electronic Health Record.- Use Secure Messaging to communicate online with your VA health care team. You may send messages to request or cancel VA appointments. Use it to ask about lab results or find out about a medication or health issue. Or simply to discuss other general health matters.

Login.gov team

Interview Objective

Understand the processes, roles, user experience, and challenges around setting up and accessing a login.gov account and the plan for the USPS pilot. In particular focusing on:

- USPS in-person proofing process
- Multi-factor authentication options and challenges
- Trusted referee options and process
- Defining access for users related to primary login.gov account holders
- Current thinking around inherited proofing from MHV

Interviewees

Annie Hirshman

Lead UX Designer

Ben Chait

Product Manager

Chanan Delivuk

Partner CX Coordinator for
login.gov

Jeff Holden

Product Manager on Partnerships
Team

Princess Ojiaku

Lead UX on Unsupervised Remote
ID Workflow

“There’s quite a bit [Veterans] have to do online before they can [...] go to the post office.”

Annie Hirshman

“Some users bounce as soon as they get to [the upload] screen. Some of the users will upload an image but never actually submit.”

Ben Chait

Login.gov - Key Takeaways

- One third of users abandon the process of creating a login.gov account, the two major drop-off points are the initial instructions and document upload
- The login.gov team does not have a good picture of the causes for failure for the document upload step, a major drop-off point in creating a login.gov account
- Low tech options are available or being explored for specific pain points in the online flow, but there is not a complete low tech or in-person option
- Trusted referee options could provide proof of identity for those who do not have approved ID or an address
- Security key are easy to use and provide the highest level of security but they are unfamiliar and require initial setup and thus the least used
- The MFA options that are most commonly selected (codes, SMS, face/touch) are those that can be done instantly, but are not universally accessible and can result in security issues