VA IDENTITY PRODUCT

Sprint 4 Demo

Wednesday, October 12, 2022

VA | U.S. Department of Veterans Affairs

MOVE

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

Tyler Gindraux
Sr. UX Researcher, Key Personnel

Joining next week! 🎉

Executive team

Jeff Scheire
MO Studio

Travis Hoffman
MO Studio

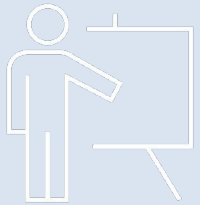
Kevin London
frog Design

WELCOME TO THE SPRINT 4 DEMO

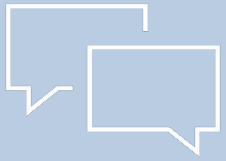
At the end of each sprint on Wednesday, the team will run sprint reviews to showcase the sprint's work for approval.

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

Sprint 4 goals

- ✅ VFS Platform orientation (outside of scheduled OCTO-req'd trainings)
- ✅ MHV Coordinator focus group #2
- ✅ Non-Veteran working group session (with Carnetta, Melissa, and Laurie)
- ✅ Prep for field research
  - *Research Plan & Discussion Guides Created & Reviewed*
- 🚧 Collaboration Cycle: Jumped to Research Steps
  - *Prepped for Research Review (submitting October 12th)*

Today’s agenda

10 min	Program status
20 min	Stakeholder interviews: *MHV Coordinators and overall key themes*
10 min	Security keys generative research
10 min	Non-Veteran user roles
10 min	Data input analysis & migration options
15 min	Field research plan
5 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 is required to meet Login.gov standards. The end goal is to simplify the migration process for existing users.

Priority 4

Security keys as an MFA option distributed during in-person proofing

Some users struggle with using Multi-Factor Authentication. Could MHV Coordinator 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

1. Carnetta Scruggs: MHV
2. Sonja Skinner: MHV
3. VSP Team: Account Migration
4. Dr. Carla Hill: TAP
5. Melissa Rebstock: VBA, VBO
6. Dr. Berkowitz: Data and Ethics
7. Matt Baum: Health Data Security
8. Coordinators Focus Group #1: MHV
9. **Coordinators Focus Group #2: MHV**
10. **Non-Veteran Working Session**

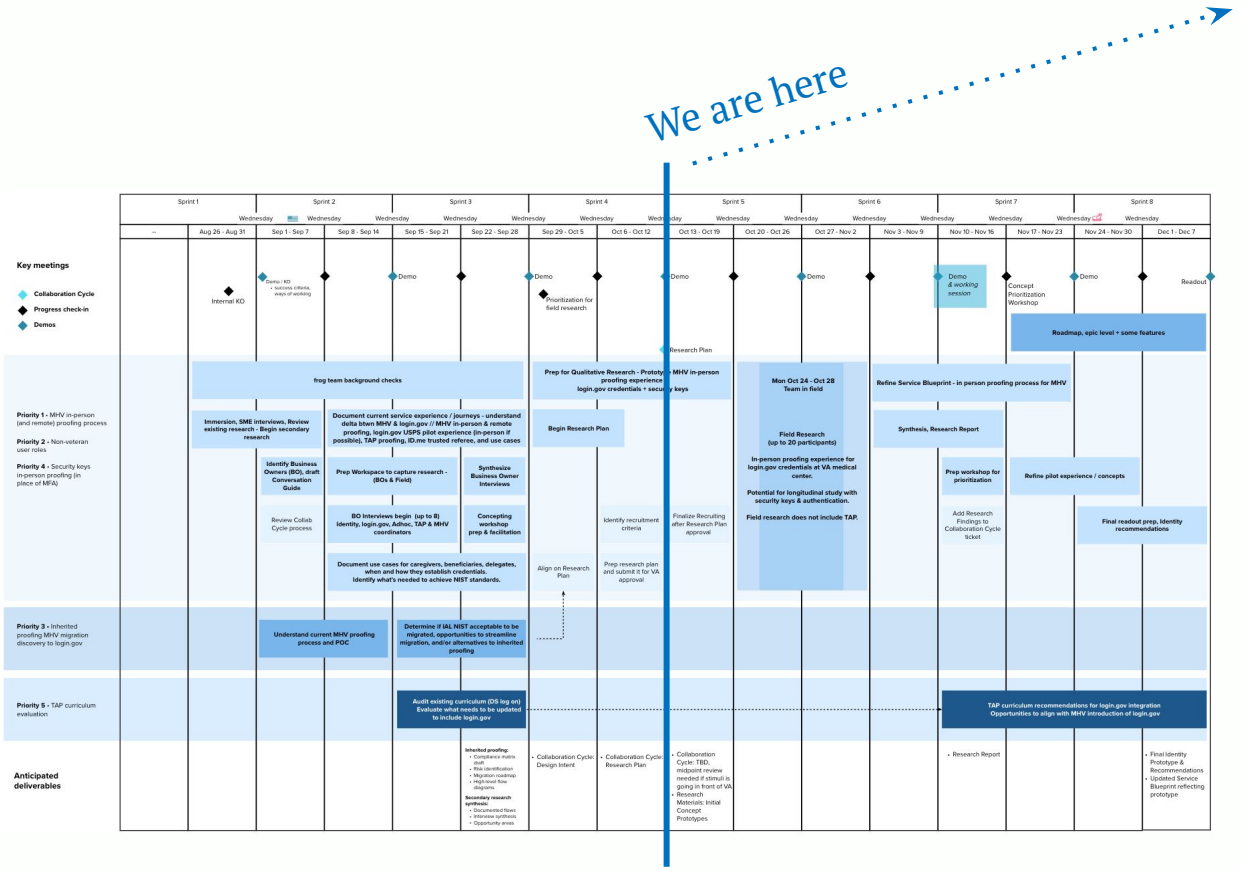
Upcoming interviews

11. Laurie Baker: VBA, VACO
    - *Senior Management Analyst*
    - *Wednesday, Oct 12*
12. Danny Reed: VHIC subject matter expert
    - *Friday, Oct 14 (tbd on exact timing)*

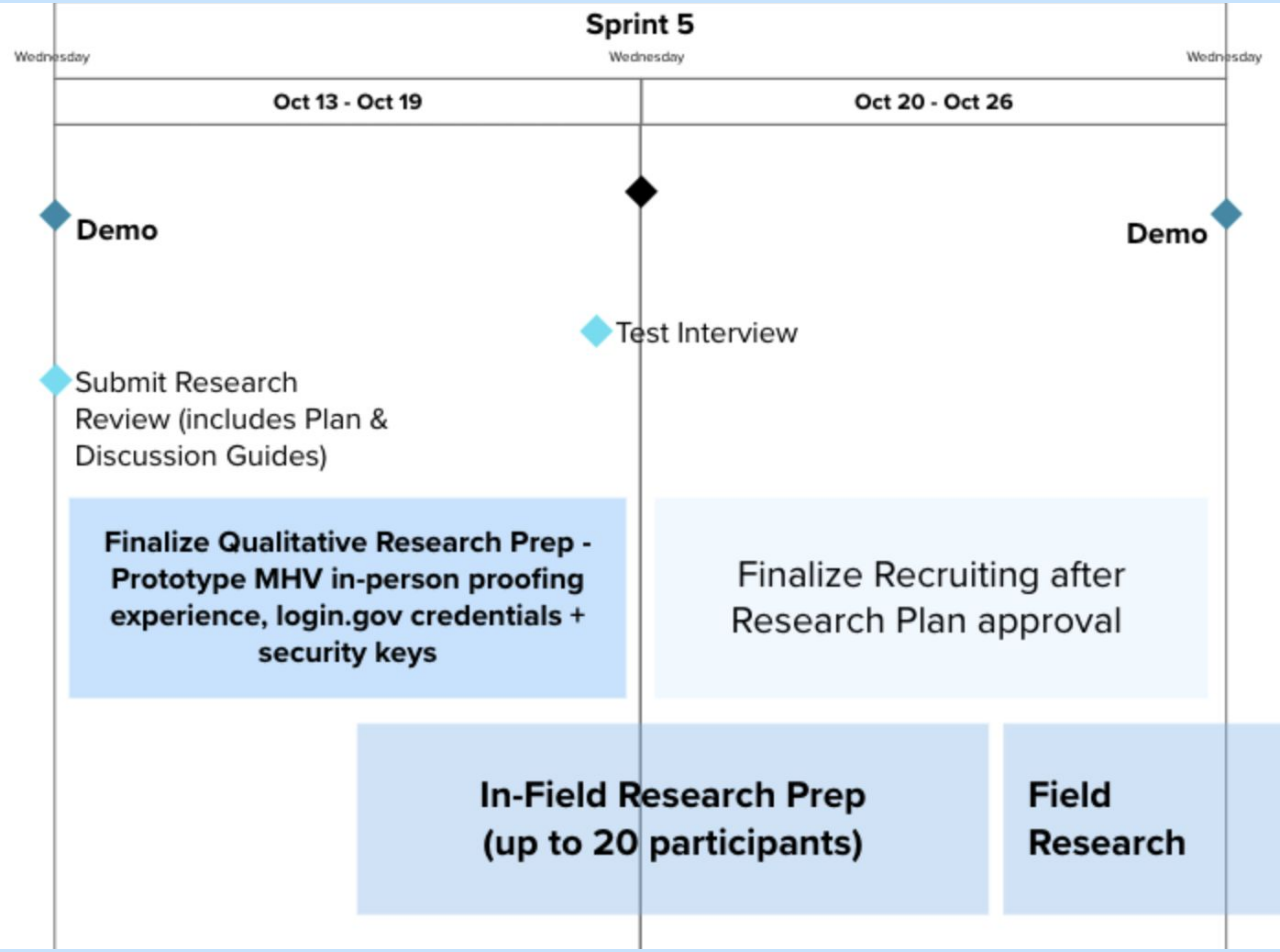
On hold

N/A

Our plan



A closer look to the sprint ahead...



Dependencies, risks, blockers

Dependencies:

- Peregian recruiting, which impact
  - Field research locations & approvals
  - Finding contacts at selected VAMCs to coordinate with
  - Travel Planning
- Research Review & Approval (10/14 absolute latest to submit)

Risks:

- Ability to recruit desired participants between 1-3 locations for in-person interviews

Blockers:

- VA larger file & videos access (requires google access)
  - Granting ability to get PIV card & reader, should not be an issue moving fwd

What we've learned so far

Stakeholder interviews

- MHV Coordinator group sessions
- Key themes emerging from all stakeholder interviews

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 Conducted

Session 1

5 - MyHealtheVet Coordinators
Monday, September 25, 2022

- Lolita Price (Alabama)
- Philip Walton (Iowa)
- Melissa Beals (Alaska)
- Dwayne Cunningham (Montana)
- Renee Ruggles (Nevada)

Session 2

3 - MyHealtheVet Coordinators
Monday, October 3, 2022

- Ramona Dewitt-Morris (West Virginia)
- Alane Wright (Florida, Georgia)
- Marcus Mallette (Gulf Coast)

MHV Coordinators: Key takeaways

1. The fear of losing access to MHV and the hassle of trying to set up new credentials take a huge emotional toil. Veterans do not understand why this is necessary and react with anger and frustration.

2. Generational differences in life and technology practices are overlooked in service design and digital experiences (e.g., shared emails, no driver's license, preference for phone help, general distrust).

3. Any change in login credentials and new proofing requirements means some Veterans will lose access—Grandfathering must be considered to avoid leaving Veterans behind.

"We're leaving a generation behind."

Dwayne

"[A Veteran said to me] 'They trusted me with nuclear codes but they don't trust me with my ID.' "

Dwayne

"You have some people that don't have a driver's license because they aren't allowed to drive anymore. You've got an aging population, that needs to make sure you accept VHIC. That's what they're here for!"

Ramona

MHV Coordinators: Key takeaways

4. Even before technical challenges of migrating to Login.gov, problems of timing, unclear messaging, and triggering words confuse and upset Veterans.

5. Users get lost in the process of registering and authenticating due to a disjointed flow and poor visual hierarchy. On the back end, system logic does not match how users actually use MHV resulting in accounts being deactivated, which blocks upgrade/setup.

6. MHV Coordinators and their authenticators do not have sufficient visibility into the process or access to VA-specific support to troubleshoot the myriad of issues that may be blocking a Veteran from successfully creating a Login.gov account.

“When you're saying you're upgrading something, a lot of the Veterans feel they that they're gonna have to pay for that. I actually got chewed out just last week about, ‘how dare you make me pay…’”

Melissa

“If we can't see and troubleshoot where exactly the problem is, there should be some way that we can make it a positive end result, but we can't.”

Dwayne

MHV Coordinators: Key takeaways

7. MHV Basic provides very little value and creates an unexpected and confusing additional step.

8. The Login.gov ID recognition process for online proofing is a failure point for Veterans of all ages and levels of technical proficiency.

9. Veterans and MHV Coordinators distrust ID.me because of its commercial ties, and are angered when it seems they are being forced to use it to upgrade. Some MHV Coordinators are frustrated that Login.gov is not the highlighted option, while ID.me is labeled “recommended”.

“With the basic account you can’t really do anything.”

Phillip

“I’ve had an actual professional photographer take photos of his ID with his professional camera, upload them and they would not be accepted. He actually gave up on the process.”

Melissa

“[ID.me has] been a continuous nightmare that I can’t wake up from.”

Phillip

MHV Coordinators: Key takeaways

10. Even technologically-challenged Veterans see immense benefit in MHV digital services and want a trusted, tech-savvy intermediary to assist.

11. Despite the frequency with which Veterans rely on a caregiver to help them access MHV, getting the caregiver officially recognized with their own account will be a challenge because just using the Veteran's credentials is so easy and familiar.

12. Digital MFA options are not understood by older Veterans. Although physical security keys may address some problems, MHV coordinators fear they will be frequently lost.

"90% of Veterans want access to MHV just to access their medications."

Marcus

"[Caregivers are] not gonna take the time to put their information in in order to get their dad's health records when they've been [signing in with their dad's credentials] for years."

Ramona

"No one wants to hang on to a device. Veterans are 'old-school', we can't rely on something that can be lost."

Ramona

Overall: Key themes that are emerging

From 10 stakeholder sessions conducted that spanned TAP, VBO, MHV, and ethics of security & compliance

1. **No Veteran left behind**
   Any change to login credentials and proofing requirements means some Veterans will lose access—We need to solve for the hardest to reach Veterans (rural, homebound, or unwilling to alter their digital practices), and expect serving them will require special accommodations and additional resources, including grandfathering some into Login.gov.

2. **Login is an emotional issue**
   Login requirements are not merely an intellectual question of data security for Veterans. They can be life-or-death issues of being able to access their prescriptions, shame with personal limitation, as well as a betrayal of trust when they feel the VA is not providing what they have earned or that their personal information is being shared inappropriately.

3. **Piece-meal doesn’t work**
   Point-solutions to technical issues related to MHV and Login.gov will not create a truly accessible solution. To serve all Veterans a holistic approach to the entire login process that includes not just addressing technical challenges, but also considers messaging and process is required.

4. **Simplify, simplify, simplify**
   The combination of multiple account types, multiple ways to login, and circuitous flows between them creates unclear expectations and confusion. Eliminate MHV basic, make a clear recommendation for login, and eliminate unnecessary signing into and out of accounts.

5. **We’ve already done this**
   From enlisting onward, Veterans provide a lot of information and fill out a lot of forms. There is an opportunity to repurpose this data and these processes to minimize the frustration of migrating to Login.gov.

Overall: Key themes that are emerging

From 10 stakeholder sessions conducted that spanned TAP, VBO, MHV, and ethics of security & compliance

6. **The buck stops with MHV Coordinators**
   MHV Coordinators do not want to turn Veterans away without a solution. Until they have more visibility and education about the process and direct access to support, they will avoid recommending Login.gov and will bend proofing rules to ensure Veterans can access MHV premium.

7. **One size does not fit all for MFA**
   The current MFA options will make Login.gov inaccessible for some Veterans. Support for using security key, enabling data from a VIC or VHIC to act as additional verification, as well as the possibility of waiving MFA protection altogether must all be explored. The right balance of security and ease of access will vary depending on the Veteran.

8. **Offer incentives and easy undo, not double confirm**
   Caregivers (official and unofficial) and delegates are essential to the VA delivering the services it owes Veterans. Registering with the VA as a caregiver must provide additional value not available by simply using the Veteran's account, and VA systems must provide fail-safes and realistic policies given Veterans will share their credentials.

9. **An ounce of prevention is worth a pound of cure**
   TAP curriculum is one of many places where streamlining the recommendation for login and providing consistent training could prevent confusion and additional effort down the line.

Security keys, generative research

Generative research objective: Currently, stakeholders and business owners we have spoken with are widely unfamiliar with security keys and are not trying to provide keys to Veterans as an MFA option where it exists (e.g. Login.gov). This research aims to understand if, how, and for whom, the introduction of security keys would be feasible and effective MFA option to offer and promote.

We compared the top security keys on the market, and **Yubikey** and **Titan** keys have the highest potential to meet a wide range of Veterans' user needs

Current Popular Products

Notable Features

- Single / pairs
- Button
- Nano
- Multiple Accounts

Security Standards

- NIST
- FIDO
- Most secure MFA

Influential Clients / Promoters

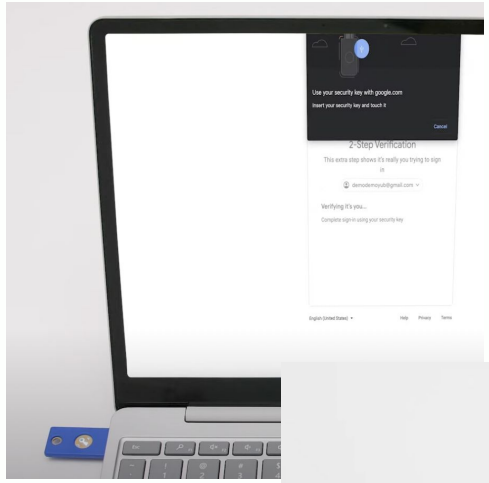
- Tech:
  - Google, Microsoft, Amazon
- Finance:
  - JP Morgan
- Political:
  - Defending Digital Campaigns (DCD)

Cost

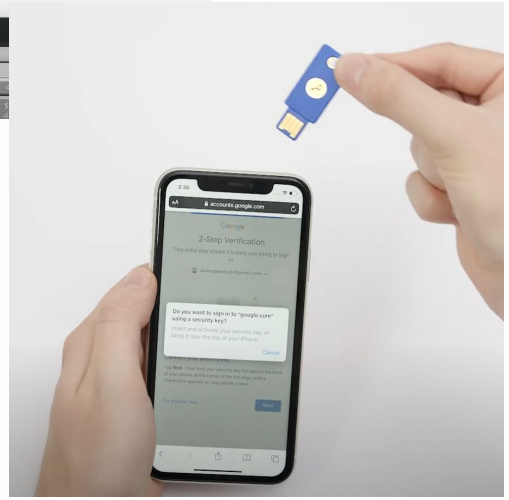
- $25–70

Sources: Yubikey for Federal Government | NYT: The best security key for MFA | SC Magazine: Tech giants encouraging adoption of hardware-based auth keys | SC Magazine: Biden signs massive cyber order… | CNBC: Amazon Web Services will give free USB security keys…

The process to set up and use security keys is a simple, self-contained option in comparison to other MFA options



Desktop



Mobile

Ordering

Online: Amazon, direct company websites, Google store

Setup

1. Prompt to set up MFA
2. Select security key option
3. Tap/Plug in & click

**Varies by provider*

Use

1. Login with username/password
   - *Some might not require this based on IT configuration*
2. At MFA page, tap/plug in & click

Loss / Replacement

1. De-associate key
2. Direct users to other MFA options while waiting for replacement **or** use backup key

**Can re-associate original key if found*

Sources: Instructional Setup Series: YubiKey Security Key Series | How to Geek -What to do if you lose a U2F key | The Verge- ou can now sign into a Microsoft Account without a password with a security key

Understanding general trends in these demographic subcategories allows us to estimate Veteran user population sizes and consequent impact when addressing those populations' needs

Age & Location

- >70% urban regardless of age
- No major difference in age composition between rural and urban

Trust & Tech Footprint

- General trend of increasing trust in VA (79%)
- War = erosion in trust, (i.e., Vietnam Veterans)

Smartphone Ownership

- Ranges from 47-76%,
- Lowest ownership & connectivity/financial barriers were rural & older

Age

- 25-34 & 65+ most likely to use VA benefits

Caregiver Use

- Roughly 1 in 3.5 Veterans have a caregiver

Homelessness

- In US, declined by 50% since 2010
- In 2020, 21 of every 10,000 Veterans in the US were experiencing homelessness (<1% of entire Veteran population)

Sources: National Center for Veterans Analysis and Statistics: Veteran Population | Veterans' Attitudes Toward Smartphone App Use Health Study | Federal News Network: VA Trust Article | Washington Post: War Bequeaths a Distrust of Government | Rand Corporation: Military Caregivers Article | National Alliance to End Homeless: How many Veterans experience homelessness? | Military Times-The number of veterans experiencing homelessness..

We identified 9 potential use cases for security keys, 5 of which likely have an immediate need for this MFA option

Why do people need a security key in lieu of other MFA options?	How will those needs be met?	Which are the types of VA users that could have this need?	To what extent is this user underserved today?	What is the size of estimated of VA user base fits in this category?	Should the VA invest in security keys for this need?
Have an MFA option that does not require a smart phone	verify identity over the (dumb) phone easily identify via web browser addresses connectivity issues	Older (65+) Unhomed Unlikely to have own smartphone Rural	Moderately served Current solution (pic upload) with frequent issues exists, does not require a smart device	Population Size: Large The rate of smartphone ownership reported by veterans ranges from 47% to 76%.	No, the pre-existing non-smart phone MFA option through email addresses these main user needs sufficiently.
Have an MFA option that does not require accessing other websites/accounts	provide a log-in experience that includes extra educational support verify identity over the (dumb) phone addresses connectivity issues	Older (65+) Rural Unlikely to have own smartphone Requires simplicity	Underserved All current solutions require using other apps/ sites	Population Size: Large Approximately 5M veteran users are based in rural areas with about half of them being above age 65.	Yes, an MFA option that is a one stop shop would be significant for many hard-to-engage users including those with low bandwidth in rural areas, limited mobility/dexterity, lack of technology access/familiarity.
Have an MFA option that has fewer steps	Have a 1-stop shop digital experience addresses connectivity issues	Older (65+) Rural Requires simplicity Potential physical limitations	Moderately served Multiple current MFA options require <10 steps	Population Size: Large	
Have an MFA option that does not require refined movements	login experience requires as few to no time sensitive methods Login experience that limits required typing elements	Older (65+) User with a caregiver Potential physical limitations	Underserved Nothing currently offered is as simple as a button press	Population Size: Small Of the data available, the higher the disability rating, the higher the likelihood of being an engaged user of VA health care (as high as 90% engagement of a disability-rated group)	Yes, currently all MFA options offered require a typing or time-sensitive element in comparison to a simple button press.
Have an MFA option that does not require any travel even for set up	Can be set up remotely easily Comes set up tutorial documents If a required physical item, it can be mailed	Older (65+) Rural Potential physical limitations	Moderately served All elements can be mailed Set up is relatively simple in comparison to app downloads or email logins	Population Size: Medium	No, for those who will always need tech handholding we cannot guarantee they won't have to travel for assistance.
Reduce feeling that govt is tracking user through a network of devices/accounts	includes educational materials on what data is stored Includes educational materials on comparative levels of security	Older (65+) Rural Selective user of Veteran benefits/ networks	Underserved Other options require some connection between devices/ accounts; this is the only potential solution that does not link in this way	Population Size: Small Trust in the VA is increasingly on the rise, so % of veterans concerned with tracking/trust in institutions is lower	Yes, this smaller population is the hardest to engage, so the VA needs a strategy to engage them while maintaining their need to feel safe/independent.
Feel like sensitive information is as secure as possible	Includes educational materials on comparative levels of security includes educational materials on what data is stored	Older (65+) Potentially has background in data security Security sensitive	Moderately served Processes currently in place work to ensure data storage/use is secure and not left vulnerable	Population Size: Medium	No, currently factors like accessibility and delegation capabilities seem like the top priorities to address.
Eliminate all potential phishing risks	Includes educational materials on comparative levels of security	Potentially has background in data security Concerned about scams Security sensitive	Underserved Phishing is not at the forefront of security concern Primary concern is ensuring that the Veteran is who they say they are	Population Size: Small	No, phishing is not a top priority for our stakeholders/ business owners thus far.
Feel like they have final say over who/when accesses their account	have 1 easy to use device that is the final say to access	Older (65+) User with a caregiver Unlikely to have own smartphone	Underserved Most caregivers informally use veteran's login info, giving them full access to all veteran's info Other MFA options like OTP apps live on caregiver's phone	Population Size: Large Roughly 1 in every 3.5 veterans has a caregiver	Yes, giving veterans control of the final step for caregiver access to veteran's accounts would empower veterans, while a more formalized delegation system is determined.

Let's take a closer look…

A closer look...

Why do people need a security key in lieu of other MFA options?	Can security keys significantly help these users who struggle with MFA?
Have an MFA option that does not require a smartphone	No, the preexisting non-smart phone MFA option through email addresses these main user needs sufficiently.
Have an MFA option that does not require accessing other websites/accounts	Yes, an MFA option that is a one-stop-shop would be significant for many hard-to-engage users including those with low bandwidth in rural areas, limited mobility/dexterity, lack of technology access/familiarity.
Have an MFA option that has fewer steps	
Have an MFA option that does not require refined movements	Yes, currently all MFA options offered require a typing or time-sensitive element in comparison to a simple button press.
Have an MFA option that does not require any travel even for set up	No, for those who will always need tech hand holding we cannot guarantee they won't have to travel for assistance.
Reduce feeling that govt is tracking user through a network of devices/accounts	Yes, this smaller population is the hardest to engage, so the VA needs a strategy to engage them while maintaining their need to feel safe/independent.
Feel like sensitive information is as secure as possible	No, currently factors like accessibility and delegation capabilities seem like the top priorities to address.
Eliminate all potential phishing risks	No, phishing is not a top priority for our stakeholders/business owners thus far.
Feel like they have final say over who/when accesses their account	Yes, giving Veterans control of the final step for caregiver access to Veteran's accounts would empower Veterans, while a more formalized delegation system is determined.

Additional considerations

Opportunities

- Easy set-up
- Rising in popularity
- Physical solution may resonate with older generations
- Highly secure
- Limited mobility or limited tech-friendly
- Backed by credible organizations
- Provides login step that Veteran can control each time a non-Veteran user logs into their account

Challenges

- Can be expensive
- Suggested to have multiple keys
- Potential USB incompatibility
- Can be lost or not with user when needed
- Current limited knowledge from staff & users
- Some keys require a PIN

Security Keys: What's next?

- Connect with Login.gov/GSA on current security key processes
  - What resources/education they provide upon distributing security keys today
  - Cost estimates and responsibility
  - Current path to recovery/replacement
- Explore strategies for MHV Coordinator/Benefit Advisor buy-in
  - Security key training materials
  - Distribution among staff to drive familiarity and consequent promotion
- Determine future path for research and testing adoption
  - Messaging and training material to facilitate self set-up of security keys
  - Providing a security key and supporting set-up as part of TAP
  - Pilot distribution of security keys and longitudinal study to monitor usage

Non-Veteran user roles

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 definitions of these users or **clarity on their use cases and needed levels of access**.

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

Work to-date

Completed

- Completed & integrated notes primarily from the MHV and TAP-focused interviews
- Reviewed the Non-Veteran User Roles Discovery Readout and supporting research
- Conducted additional definition session with Melissa Rebstock and Carnetta Scruggs
- Secondary research outside of VA-produced materials
- Reviewed the MHV delegation research materials provided by Carnetta and the MHV team

In-progress

- 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

High-level themes/needs

Stakeholders agreed on:

- Non-Veteran user type does not indicate required level of access, however, there is a need for tiered access for both privacy and relevancy according to role
- Programs warrant a need to reflect changes to Veterans' relationships and care needs which can be done via a non-Veteran user renewal process
- A single source of truth for non-Veteran user role profiles—integrated with all the VA applications that warrant access—would allow Veterans to control how and what information is being accessed
- Given non-Veteran users have similar responsibilities, questions, and needs as other non-Veterans and Veterans alike, they should also have access to a helpdesk
- A standardized process for non-Veteran user registration that's dependant on user type/access need would satisfy VA staff need for user recognition and tracking
- Non-Veteran users acting solely as beneficiaries should not be part of conversation regarding access to Veteran information, unless they are involved in Veteran care and are therefore another user type

Stakeholders disagreed on:

- Confusion and disagreement amongst user roles, about their definitions, and use cases present a need for the following:
    - Universally agreed upon non-Veteran user definitions
    - Shared education about the roles and official terms of use
    - Collective understanding that a caregiver must be officially recognized/registered

Caregiver, as previously defined

However, the sentiment from working session was that caregivers should always be officially recognized and that the term caregiver often acts as an umbrella term.

Research Findings

A Veteran's **caregiver** is a person who provides support to the Veteran. Caregivers could be individuals who are officially recognized by the VA, self-identified individuals, or professional caregivers.

- VHA has specific programs to recognize caregivers; the programs have specific eligibility criteria.
- Caregivers participating in the VA Comprehensive Assistance for Family Caregivers Program (PCAFC) would also be beneficiaries since they receive direct payments from VA.
- There are a couple of existing channels for self-identifying caregivers to have access to Veteran information: VA Online Health Delegate Program, and the VA Fiduciary Program
- There aren't any clear rules about whether a caregiver should be allowed access to a Veteran's information; it's generally determined on a case-by-case basis.
- Read finding 3 in the full report for additional details on caregivers

Source: VA's 2021 Non-Veteran User Roles Discovery Readout

Caregiver

Veteran users	Role definition	Colloquial use of terms	Needed products / Services / Deliverables	Use cases (revealing varied levels of access)
Any Veteran can have a caregiver whether they have a rated disability or just prefer to have their spouse/child/ friend type for them	• Must be officially recognized by VA in VistA • Is a beneficiary if officially VA recognized • Is not necessarily the PoA or legal guardian • Includes current understanding of unofficial delegate/ health care proxies • Varies by organization (VBA, VHA) • Can be the primary and secondary caregivers **Can include Fiduciaries, Surrogates, Power of Attorneys, or Legal Guardians** A federal fiduciary is a person or legal entity authorized by VA to serve as payee of VA benefits for a beneficiary unable to manage his or her financial affairs. • A court-appointed fiduciary is a person or legal entity appointed by a state or foreign court to supervise a beneficiary unable to manage his or her financial affairs and/or that person's estate.	• Officially or unofficially recognized • Anyone who is a trusted intermediary at all involved in Veteran care • Does not necessarily have their own account	• Develop a caregiver renewal process • Standard form of ingesting information to authorize Caregivers • Quick non-Veteran user recognition and profile verification	• Transportation (when & where are appointments) • Prescription refills • Messaging health care providers on Veteran's behalf • Scheduling appointments • Assisting a Veteran with filing a claim for benefits • Manage monetary benefits • Participate in / are responsible for medical decisions

Delegate, as previously defined

The term delegate elicited strong reactions from our working sessions- users were quick to correct us that the more recognized term for how we have been using delegate is health care proxy, and that official delegates only come into play when Veterans are determined incompetent.

Research Findings

A **delegate** role exists in VHA to refer to someone who has delegate authority per the request of a Veteran through the VA online health delegation program.

- VBA does not have a specific delegate role. There is a VBA process through VA Form 21-0845 that gives a 3rd party access to information for a Veteran.
- A delegate does not have to be a dependent or a beneficiary.
- Delegates can directly access some Veteran health information online, such as upcoming appointments and prescription information, in MHV and participating VA Mobile Apps. More information can be found in finding 3.4 from the first phase of our research.
- A delegate cannot help a Veteran with offline health tasks.
- A VA recognized Caregiver and a Delegate would likely need to be two different types of access on VA.gov since a VA recognized Caregiver is also a beneficiary that would need to see information about their own benefits.

Source: VA's 2021 Non-Veteran User Roles Discovery Readout

Delegate

Veteran users	Role definition	Colloquial use of terms	Needed products / Services / Deliverables	Use cases (revealing varied levels of access)
Veteran is deemed "incompetent" (by VA or under legal disability by reason of court action) A mentally incompetent person is one who because of injury or disease lacks the mental capacity to contract or to manage his or her own affairs, including disbursement of funds without limitation.	• A delegate acts on behalf of a Veteran deemed "incompetent" or "insane" by the VA for financial, medical, legal, and other benefits related purposes • Adhering to all responsibilities held by the Delegator • No official role recognized by VBA	• Many refer to unofficial delegates as healthcare proxies	• Ability for delegate to act as head point person and appoint additional caregivers as needed. • Quick non-Veteran user recognition and profile verification	• Greatly overlaps with caregiver use cases (appointments, prescriptions etc.) • Potential to need to know everything about the Veteran's health

Beneficiary, as previously defined

Research Findings

A **beneficiary** is anyone who is the direct recipient of a benefit or service from VA.

- In VBA, the term is also used to refer to a person the Veteran has named to receive their benefit in the future.
- A beneficiary could be a Veteran, or a qualifying family member.
- Each benefit has specific qualifications to determine beneficiary eligibility.
- The tasks a beneficiary would need to do on VA.gov are the same for Veterans and non-Veterans. For example, a non-Veteran beneficiary receiving education benefits should be able to update their direct deposit information or view payment history the same way a Veteran would.
- A beneficiary isn't always a dependent. E.g. VA recognized caregivers who are not dependents.
- Beneficiary data currently lives in the VA Corporate Database (sometimes called CorpDB), and is correlated to the Veteran file number. Efforts are currently underway to add a beneficiary PERSON_TYPE to MPI.

Source: VA's 2021 Non-Veteran User Roles Discovery Readout

Beneficiary

Veteran users	Role definition	Colloquial use of terms	Needed products / Services / Deliverables	Use cases (revealing varied levels of access)
Any Veteran with benefits	• A beneficiary is an individual entitled to receive VA benefits. Beneficiaries are classified as minors, Veterans, and other adults. The latter group includes adult children incapable of self support, surviving spouses, dependent parents, and some insurance payees. • Any person(s) defined by Veteran • Often parent/ spouse/ family member of non-Veteran use • Can be an officially recognized caregiver			• Does not need access to Veteran's care information if only strictly acting in this role/ to receive benefits • Only need access to their own benefit information

Non-Veteran user roles: Determining what we can do now, next, and later

Open questions

- If and when should we reflect these definitions and product concepts back to Carnetta Scruggs and Melissa Rebstock?
- 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?
  - Is the intention to move forward with validation of these proposed strategies to utilizing security keys with these non-Veteran users?
- 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?)

Note: We may learn some of the above in the field depending on participants recruited, however there is likely a future need to conduct primary research with these roles & users.

Sources: VA Identity and Access Management Transmittal Sheet | VBA Definitions Site | VA Determinations of Incompetency | Business Owner Working Session with Carnetta, Melissa, & Laurie


Exploration for MHV Premium migration

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 is required to meet Login.gov standards. **The end goal is to simplify the migration process for existing users.**

Migration viability: Good news, there are ways to streamline data

We can pull the data necessary to generate a Login.gov account from a MHV account except for *ID proofing* and verifying the *address* if the phone number verification fails.

- Login.gov doesn't allow just username and password—it requires more secure means of authentication
- State-issued ID is an approved ID for MHV Proofing and a requirement for Login.gov, however not all users may be eligible if they verified via alternative means

Questions

- For migration with inherited proofing, will Login.gov accept forms of ID which are allowable for MHV in-person proofing, in addition to state-issued IDs?
- If Login.gov does not inherit the ID used to proof for MHV and requires reproofing with upload of an ID, is State-issued ID the only allowable ID type?

	MHV Basic	MHV In-Person (Requires Proofing) + Online	Login.gov (MHV Premium - Account Connecting)
Data Inputs	Name	Name	Name
	SSN	SSN	SSN
	DOB	DOB	DOB
	Sex	Sex	
	Email	Email	Email
	Phone	Phone	Phone
	User ID	User ID	
	Password	Password	Password
	Security Questions (2)	Security Questions (2)	
			Username
			Address - Not a user input
Approved IDs		**Primary IDs** >> (1 required otherwise a Secondary ID) **Secondary IDs** >> (1 required)	
		VIC	
		VHIC	
		Drivers License	Drivers License
		Passport	
		Federal, State, or Local Government-issued ID containing full name	Federal, State, or Local Government-issued ID containing full name
		Social Security Card	
		Copy of Marriage License	
		Voter's Registration Card	
		Other (i.e. Utility Bill or patient's medical wrist band)	
			Personal Indentification Verification (PIV) card
			Common Access Card (CAC)

Excel spreadsheet to be shared following demo.

Note: If you are in a foreign country and don't already have access to State-Issued ID, you must use id.me

Grandfathered access to MHV may be necessary for accounts that are ineligible for inherited proofing

Risk

MHV premium accounts that are not compliant with IAL2 (varies by account, whereby evidence was collected and verified with varying levels of compliance), **Login.gov *may* require an undesirable burden on Veterans to repeat some/all identity proofing steps**, e.g. upload of state-issued ID, SSN validation, or phone #/address validation.

Recommendation: Mitigate risk by migrating non-eligible MHV Premium accounts to Login.gov as IAL1 accounts with **grandfathered** access to MHV *(deferred Login.gov IAL2 account)*

- **Catch-all alternate solution** to migrate all MHV premium accounts, which otherwise cannot migrate via inherited proofing
- Maintain **trust of Login.gov** through NIST compliance, notably with attributing IAL2. Conversely, MHV premium accounts with non-compliant proofing evidence will remain accurately reflected as IAL1
- Grandfathering of accounts offers a **streamlined migration**, in terms of identity proofing, in that no proofing steps will be required. Ideally, inherited proofing will likewise require no additional proofing.
- With grandfathering, **proofing can be deferred** until needed. Login.gov IAL1 accounts will be reusable across government agencies, although limited access until upgraded. The limited use of IAL1 accounts across agencies will provide **additional incentive to upgrade to IAL2**
- If grandfathering is offered as an *option* to Veterans in cases where Login.gov cannot fully inherit proofing, **Veterans are empowered** with a migration alternative if the burden of reproofing is too great.

Let’s also think beyond migration and streamline the process for users who have a Login.gov account and *then* seek to create an MHV profile

Let’s remove the burden of additional username and password creation for MHV—a credential they shouldn’t ever need to use thanks to Login.gov.

Inherited proofing, what's next?

Questions

- **Login.gov**, who can clarify:
  - What is Login.gov's eligibility criteria requirements for an IAL2 account using inherited proofing?
  - Which proofing steps (State issue ID, SSN and phone #/address verification) will Login.gov forego based on inherited proofing and will this vary based on how MHV premium accounts were proofed?

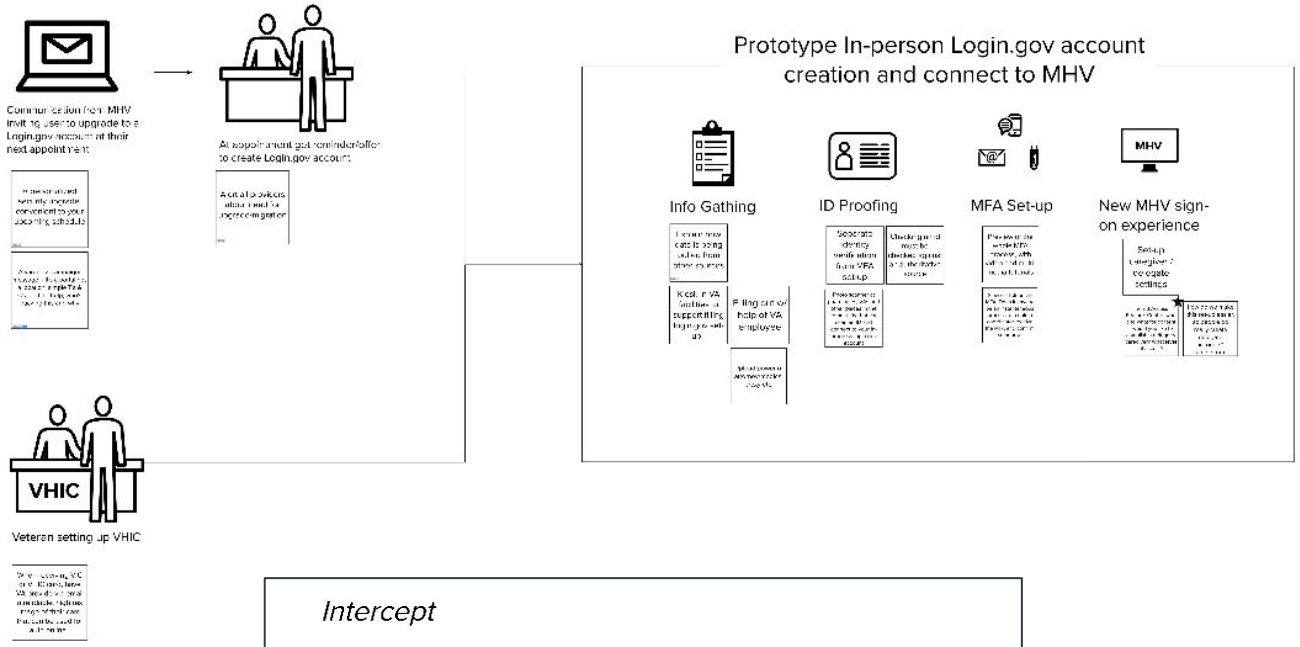
- **MHV**:
  - Can we (and the eligibility API) get access to MHV account identity verification data required to assess existing accounts against Login.gov's eligibility criteria?

So, now that we have a foundational understanding of the challenges and opportunities…

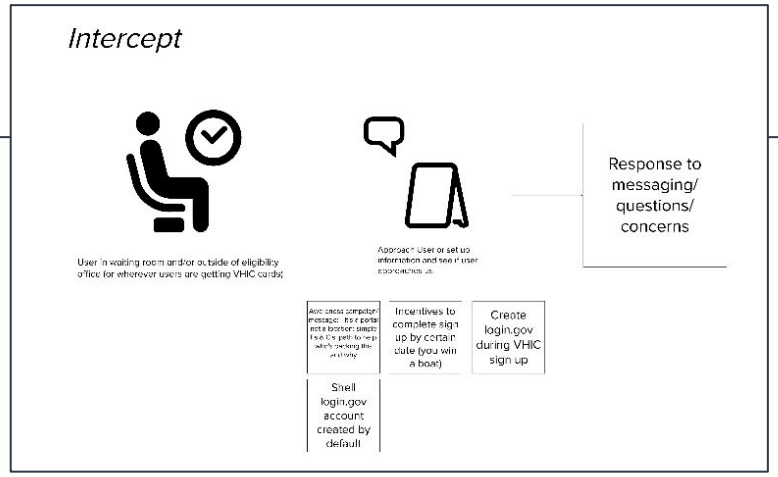
What can we test in the near-term to improve in-person proofing and set a Login.gov pilot up for success?

In-person migration & proactive account creation

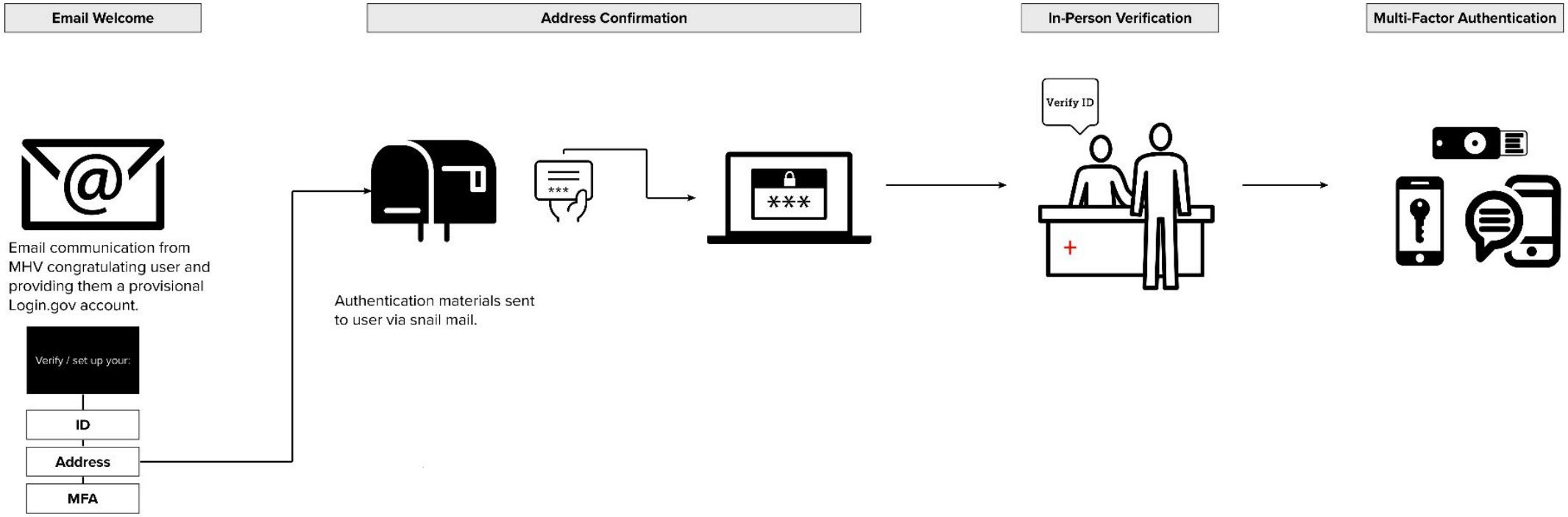
In-person account creation at VA facility



Intercept



Migration flow 2: Deferred proofing



Questions:

- Can MFA setup be deferred? Or waived?
- Is it valuable to test Veteran reaction of having an account set up on their behalf? (Do they expect to be able to consent or does it make the process feel less daunting?)
- How else can we build on this to create additional pathways to increase adoption?

Our plan for field research

Location

- Up to two (2) VAMC in different regions that serve a diverse population of Veterans including a substantial older population. A secondary priority would be to have one tier 1 and one tier 3 VAMC.

Participants

- A diverse group of 12–14 who are active MHV Premium users who do not have a Login.gov account. Ideally some or all would be Veterans who have tried and failed to set up a Login.gov account.
- A diverse group of 6–8 Veterans who do not currently have a MHV account. Ideally these users would have recently signed up for or received a VHIC.

Research Goals

- Understand how we can intervene proactively to ensure that new generations of Veterans use Login.gov or ID.me to access MHV from the beginning.
- Understand what in-person support will enable Veterans who have technical or other challenges to create a Login.gov account and use Login.gov to access their MHV account.
- Understand how security keys and other options could MFA more accessible to Veterans.

Work to-date

Mid-Sprint Review (10/5)
Discuss proposed research approach, concepts and flows. Key Feedback:

- Add deferred proofing flow

Learning from Past Research

- Met with Kristen via the Check In Team about intercept testing and working with site admin
- Met with MO's Carolyn about collaboration cycle

Initial Review with Shane (10/7)
Reviewed draft of research plan and discussion guide with Shane to confirm direction.
Key Feedback:

- Keep interviews under 90 minutes
- You are on the right track

Sprint 4 Demo (10/12)
Discuss deferred proofing flow.

Submit Research Documentation (10/12)

Next steps

Sprint 5 goals

- Upcoming interviews: Laurie Baker & Danny Reed
- Sprint 5 demo expectations
  - Sprint 5 mid-sprint will serve as lightweight demo deck
  - Sprint 6 demo will include research findings
- Field Research Approval
  - Research Plan
  - Discussion Guides
  - Research Stimuli Creation
  - Practice Internal Interview (10/19)
- Field Research!

Questions?

VA IDENTITY PRODUCT

Appendix

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 incentives 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

Stakeholder interviews

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

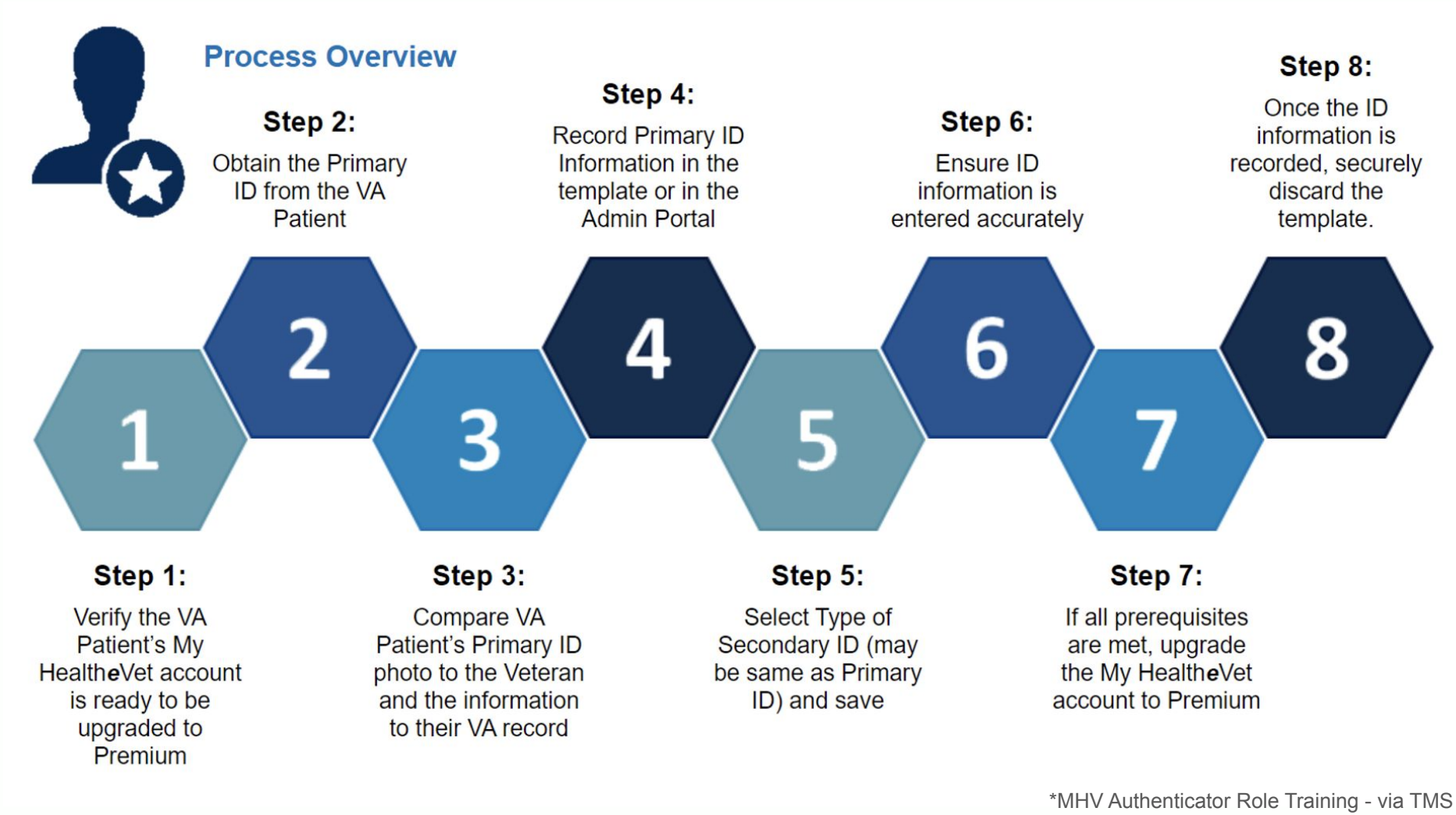
My Health*e*Vet - Key Takeaways

- 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	- 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	- Once your account is connected to your VA/DOD records, your account can be upgraded to Premium
Process	- Can be done online or in-person at VA Medical Center Online via My HealtheVet: - Complete the registration form—information collected: Name, DOB, SSN, Gender, Email Username, Password - Accept the Terms and Conditions - Select Create Your Account button	- 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	Access to your personal information located in VA or DoD systems.
	With a Basic account you may use My HealtheVet to:
	- 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:
	  - 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
		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:
		- 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
		
		In addition you may be able to:
		- 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.

MHV Focus groups

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

Carnetta Scruggs - MHV

Interview Objective

Understand the processes, roles, user experience, and challenges around setting up and accessing a My Health*e*Vet 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.

1. 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.

1. 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.

4. Partnering with USPS hopes to remove barriers and increase access for harder to reach Veterans—a benefit to both Veterans and the VA.

4. 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.

1. 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.

1. 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.

4. 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.

4. 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 for 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.

1. 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.

3. 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.

3. 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.

1. 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.

1. 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.

4. 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.

4. 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.

1. Trust is key and requires transparency, true consent, ethical use of data, and user choice.

1. 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.

4. 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.

Security & compliance assessment

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** *(Unknown, we are speculating if this option was ever allowed based on VHA policy.)*	Older MHV In-person proofing that uses **Knowledge Questions**	No ID presented	❌
USE CASE FOR MIGRATION LOGIN.GOV PILOT (VSP TEAM)			
Upgrade **In-person** *(~200,000 users)*	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

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	• Evidence validation was not performed, or validation of the evidence failed.
Weak	• All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.
Fair	• 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	• 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**
	  ○ 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).

Strength	Method(s) Performed by the CSP
Superior	• 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).